



Universidad Nacional José Faustino Sánchez Carrión

**Facultad de Ingeniería Industrial, Sistemas e Informática
Escuela Profesional en Ingeniería Informática**

**Sistema de gestión de seguridad de la información y la calidad de servicio en la
Empresa Fiberlux S.A.C. – 2023**

Tesis

Para optar el Título Profesional de Ingeniero Informático

Autor

Bruselino Yunior Blas Zorrilla

Asesora

Ing. Ana Doris Magdalena Barrera Loza

Huacho – Perú

2024



Reconocimiento - No Comercial – Sin Derivadas - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Reconocimiento: Debe otorgar el crédito correspondiente, proporcionar un enlace a la licencia e indicar si se realizaron cambios. Puede hacerlo de cualquier manera razonable, pero no de ninguna manera que sugiera que el licenciante lo respalda a usted o su uso. **No Comercial:** No puede utilizar el material con fines comerciales. **Sin Derivadas:** Si remezcla, transforma o construye sobre el material, no puede distribuir el material modificado. **Sin restricciones adicionales:** No puede aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros de hacer cualquier cosa que permita la licencia.



UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN
LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/202)

Facultad de Ingeniería Industrial, Sistemas e Informática
Escuela Profesional de Ingeniería Informática

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	DNI	FECHA DE SUSTENTACIÓN
Blas Zorrilla, Bruselino Yunior	44946838	31-05-2024
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	DNI	CÓDIGO ORCID
Barrera Loza, Ana Doris Magdalena	15727274	0000-0001-8296-6519
DATOS DE LOS MIEMROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA DOCTORADO:		
APELLIDOS Y NOMBRES	DNI	CODIGO ORCID
Huamán Tena, Ángel	15644224	0000-0003-2658-9266
Arévalo Flores, Henry Marcial	15723233	0000-0003-2958-9464
Alcántara Paredes, Ronald Eimer	17925220	0000-0002-8016-1474

Borrador Blas

INFORME DE ORIGINALIDAD



FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	11%
2	repositorio.unjfsc.edu.pe Fuente de Internet	4%
3	repositorio.uho.edu.cu Fuente de Internet	4%

Excluir citas Activo
Excluir bibliografía Activo

Exclude assignment template Activo
Excluir coincidencias < 3%

ASESOR Y MIEMBROS DEL JURADO



PRESIDENTE

Ing. Ángel Huamán Tena



SECRETARIO

Ing. Henry Marcial Arévalo Flores



VOCAL

Ing. Ronald Eimer Alcántara Paredes



ASESOR

Ing. Ana Doris Magdalena Barrera Loza

DEDICATORIA

Esta tesis se la dedico de todo corazón a mi madrecita Heraclia, quien con su esfuerzo y sabias palabras me animo lograrlo.

A mi padre Pedro y a mis hermanos quienes también me apoyaron en todo.

También se la dedico a mi amada esposa Mistrely a mis hijos Rebeca, Raquel y Daniel que son mi mayor motivación.

AGRADECIMIENTO

Las gracias sean a Dios por darme la vida, la salud y la oportunidad de concluir esta tesis.

Agradezco también a mi esposa por apoyarme diariamente para la elaboración de la tesis.

Agradezco a mis padres, hermanos y a todas la personas directas e indirectas que de una u otra forma contribuyeron a la elaboración de esta tesis.

Agradezco a todos mis maestros quienes con su esfuerzo me enseñaron y compartieron sus conocimientos para mi desarrollo profesional.

Y por último agradezco a la facultad de ingeniería, industrial, sistemas e informática por haber forjado en mi profesión.

ÍNDICE

DEDICATORIA	iii
AGRADECIMIENTO	iv
ÍNDICE	v
ÍNDICE DE TABLA	ix
ÍNDICE DE FIGURA.....	ix
RESUMEN	xi
ABSTRACT.....	xii
INTRODUCCIÓN	1
Capítulo I. Planteamiento del problema.....	3
1.1. Descripción de la realidad problemática.....	3
1.2. Formulación del problema	5
1.2.1. Problema general.....	5
1.2.2. Problemas específicos.....	5
1.3. Objetivos de la investigación	5
1.3.1. Objetivo general	5
1.3.2. Objetivos específicos	5
1.4. Justificación de la investigación	6
1.4.1. Justificación práctica.....	6
1.4.2. Justificación teórica.....	6
1.4.3. Justificación metodológica.....	6
1.5. Delimitaciones del estudio.....	7
1.5.1. Delimitación espacial	7
1.5.2. Delimitación social.....	7
1.5.3. Delimitación temporal.....	7

1.5.4. Delimitación conceptual.....	7
1.6. Viabilidad del estudio	7
Capítulo II. Marco teórico.....	8
2.1. Antecedentes de la investigación	8
2.1.1. Antecedentes internacionales	8
2.1.2. Antecedentes nacionales	11
2.2. Bases teóricas.....	13
2.2.1. Sistema de gestión de seguridad de la información (X).....	13
2.2.2. Calidad de servicio (Y)	23
2.3. Definiciones de términos básicos	30
2.4. Formulación de las hipótesis.....	33
2.4.1. Hipótesis general	33
2.4.2. Hipótesis específica	33
2.5. Operacionalización de las variables.....	33
Capítulo III. Metodología	36
3.1. Diseño metodológico	36
3.1.1. Método de la investigación	36
3.1.2. Diseño de la investigación	36
3.1.3. Tipo de Investigación.....	36
3.1.4. Nivel de Investigación.	37
3.2. Población y muestra.....	37
3.2.1. Población.....	37
3.2.2. Muestra.....	38
3.3. Técnicas e instrumentos para la recolección de datos.....	39
3.3.1. Técnicas	39

3.3.2. Instrumentos.....	39
3.4. Técnicas para el procedimiento de la información.....	41
3.4.1. Análisis documental	41
3.4.2. Análisis estadístico.....	42
Capítulo IV. Resultados	43
4.1. Análisis de los resultados	43
4.1.1. Tablas y gráficos de niveles de las dimensiones de la variable Sistema de gestión de seguridad de la información.....	43
4.1.2. Tablas y gráficos de niveles de las dimensiones de la variable Calidad de servicio	46
4.1.3. Prueba de normalidad	49
4.2. Contrastación de hipótesis	53
4.2.1. Hipótesis general.....	53
4.2.2. Hipótesis específica 1.....	55
4.2.3. Hipótesis específica 2.....	57
4.2.4. Hipótesis específica 3.....	59
Capítulo V. Discusión	62
5.1. Discusión de resultados.....	62
Capítulo VI. Conclusiones y recomendaciones.....	65
6.1. Conclusiones.....	65
6.2. Recomendaciones	66
Capítulo VII. Referencias.....	68
7.1. Fuentes bibliográficas	68
7.2. Fuentes hemerográficas.....	71
7.3. Fuentes electrónicas	71

ANEXOS	73
1. Matriz de consistencia.....	74
2. Cuestionario de encuestas.....	76
3. Formatos de juicio de expertos	78
4. Tabla de datos en SPSS.....	81

ÍNDICE DE TABLA

Tabla 1 Operacionalización de las variables	35
Tabla 2 Factores para el cálculo de la muestra.....	38
Tabla 3 Juicio de expertos para el instrumento	40
Tabla 4 Resumen del procesamiento de los casos del instrumento.....	41
Tabla 5 Estadísticos de fiabilidad del instrumento.....	41
Tabla 6 Niveles de Integridad de la información	43
Tabla 7 Niveles de Disponibilidad de la información.....	44
Tabla 8 Niveles de Confidencialidad de la información	45
Tabla 9 Niveles de Fiabilidad.....	46
Tabla 10 Niveles de Capacidad de respuesta	47
Tabla 11 Niveles de Tangibilidad	48
Tabla 12 Prueba de normalidad de las variables Sistemas de gestión de seguridad de la información y Calidad de servicio	50
Tabla 13 Prueba de normalidad de las dimensiones de la variable sistemas de gestión de seguridad de la información.....	51
Tabla 14 Prueba de normalidad de las dimensiones de la variable calidad de servicio	52
Tabla 15 Correlación entre ambas variables	54
Tabla 16 Correlación entre la integridad de la información y la calidad de servicio	56
Tabla 17 Correlación entre la disponibilidad de la información y la calidad de servicio	58
Tabla 18 Correlación entre la confidencialidad de la información y la calidad de servicio...	60

ÍNDICE DE FIGURA

Figura 1. Ciclo de Deming.....	15
Figura 2. Niveles de integridad de la información.....	43
Figura 3. Niveles de disponibilidad de la información	44
Figura 4. Niveles de confidencialidad de la información	45
Figura 5. Niveles de fiabilidad.....	46
Figura 6. Niveles de capacidad de respuesta.....	47
Figura 7. Niveles de tangibilidad	48

RESUMEN

Título de la investigación: “Sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023”. **Autor:** Bach. Bruselino Yuniór Blas Zorrilla. **Objetivo:** Determinar la relación que existe entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023. **Metodología:** Se utilizó el método Deductivo, porque el autor partió de aspectos genéricos para poder llegar a situaciones específicas. La investigación es de tipo Aplicada debido a que está enfocada en resolver problemas actuales y concretos los cuales previamente fueron identificados. Su diseño es no Experimental, de tipo transversal porque los datos se tomaron sólo una vez en el tiempo. El nivel de la investigación es correlacional, por lo cual el investigador midió la relación entre las variables. **Población y muestra:** La población está compuesta por 55 trabajadores los cuales están involucrados con el uso y procesamiento de la información y la muestra la formaron 49 trabajadores, **Técnica e instrumento:** La técnica empleada fue la encuesta y el instrumento utilizado fue el cuestionario el cual tiene 16 items, los datos obtenidos mediante el instrumento se procesaron en el software estadístico SPSS26.0 para poder analizarlos estadísticamente. **Resultados:** El modelo de correlación de Rho de Spearman devuelve un coeficiente de 0,780 y una significancia de 0,000 por lo que se demostró, con un 95% de probabilidad, que existe una correlación positiva alta entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Palabras Claves: Sistema de gestión de seguridad de la información, calidad de servicio, Integridad de la información

ABSTRACT

Research title: “Information security and service quality management system in the company Fiberlux S.A.C. in 2023”. **Author:** Bach. Bruselino Yunion Blas Zorrilla. **Objective:** Determine the relationship that exists between the information security management system and the quality of service in the company Fiberlux S.A.C. in 2023. **Methodology:** The Deductive method was used, because the author started from generic aspects in order to reach specific situations. The research is of the Applied type because it is focused on solving current and specific problems which were previously identified. Its design is non-experimental, cross-sectional because the data were taken only once in time. The level of the research is correlational, so the researcher measured the relationship between the variables. **Population and sample:** The population is made up of 55 workers who are involved with the use and processing of information and the sample was made up of 49 workers. **Technique and instrument:** The technique used was the survey and the instrument used was the questionnaire which has 16 items, the data obtained through the instrument was processed in the SPSS26.0 statistical software to be able to analyze them statistically. **Results:** Spearman's Rho correlation model returns a coefficient of 0.780 and a significance of 0.000, so it was demonstrated, with a 95% probability, that there is a high positive correlation between the information security management system and the quality of service in the company Fiberlux S.A.C. in 2023.

Keywords: Information security management system, quality of service, Information integrity

INTRODUCCIÓN

El presente trabajo de investigación lleva por título “Sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023”, se desarrolló para demostrar que el sistema de gestión de seguridad de la información tiene asociación con la calidad de servicio, lo que permite mejorar los procedimientos y aplicación óptima de los controles de seguridad de la información, llevándose a cabo además capacitaciones y concientización del personal acerca de la importancia del cuidado de la información; la investigación se realizó siguiendo lineamientos de investigaciones y estructura establecidos por la UNJFSC, los que se detallan a continuación:

En el capítulo I se expone el planteamiento del problema, describiéndose la realidad problemática, se formularon los problemas con sus respectivos objetivos, se expresan la justificación, delimitaciones del estudio y su viabilidad.

En el capítulo II se detalla el marco teórico el cual está conformado por los antecedentes, las bases teóricas y las definiciones de términos técnicos empleados en la investigación, los cuales sirven para un mejor entendimiento. Se incluye, además, las hipótesis y la operacionalización de las variables.

En el capítulo III se describe el marco metodológico del presente trabajo de investigación, estableciendo el método, diseño, tipo y nivel de la presente investigación. Además, se detalla la población y muestra, las técnicas empleadas para la recolección de los datos y el procesamiento de la información.

En el capítulo IV se presentan los resultados de las pruebas estadísticas utilizadas con el software SPSS 26.0 y las contrastaciones de hipótesis que determinaron el nivel de relación entre ambas variables y sus respectivas dimensiones.

En el capítulo V se expone la discusión de los resultados de la investigación y su comparación con resultados obtenidos de los antecedentes utilizados en el presente trabajo de investigación.

El capítulo VI está constituido por las conclusiones y las recomendaciones que el investigador cree que son necesarias para mejorar la situación actual de la empresa.

Para terminar, en el capítulo VII se muestran las referencias bibliográficas utilizadas como sustento a la presente investigación, las cuales fueron citadas conforme a las normas APA 6ta. edición, según el reglamento vigente.

Capítulo I. Planteamiento del problema

1.1. Descripción de la realidad problemática

En el mundo globalizado y tan competitivo a nivel empresarial en el que vivimos actualmente, hace que las organizaciones tanto privadas como públicas realicen mayores esfuerzos para seguir activas en el mercado. Gracias a los avances tecnológicos, las organizaciones han podido cambiar sus estrategias y formas de hacer negocio, lo cual ha generado muchos beneficios, además que gracias al internet se tiene un contacto más cercano y brindan servicios de mejor calidad a sus clientes, pero también la tecnología les está permitiendo poder asegurar su activo de más valor como lo es la información, asegurando su integridad, confidencialidad y disponibilidad.

Las organizaciones, al incrementar la utilización del internet en sus procesos de negocios, se vienen enfrentado a más riesgos debido al aumento de nuevas amenazas que provienen de diversas fuentes y formas, como fraudes informáticos, virus informáticos, ataques de intrusión, etc., lo cual genera pérdida, robo y destrucción de información. Además, deben tener en cuenta que no solo se enfrentan a amenazas externas, sino también a amenazas internas ya sea voluntarias o involuntarias como es el error humano, afectando a la organización y, por ende, afectando la continuidad de los servicios brindados a sus clientes, obteniendo pérdidas económicas.

Por otro lado, tenemos a la calidad de servicio conocido como QoS por sus siglas en inglés (quality of service) se refiere al uso de tecnología para proporcionar servicios estables que sean utilizados por sus empleados y clientes. Si estos servicios no son confiables o no existe una rápida capacidad de respuesta ocasiona que las relaciones con los clientes y empleados estén en riesgo. Hay que agregar que, si la calidad de servicio es deficiente compromete a la integridad y seguridad de la información, todo esto obliga a que toda

organización pública o privada tenga que asegurar su información mediante un sistema de gestión de seguridad de la información, el cual debe someterse a una mejora continua actualizando sus políticas de seguridad, controles y procedimientos, debido a que los delincuentes informáticos vienen actualizando las maneras y herramientas utilizadas para cometer sus delitos.

La empresa Fiberlux S.A.C. no cuenta con un sistema de seguridad actualizado que cuide el almacenamiento, procesamiento y manejo de la información, la cual ha ido incrementándose en los últimos años. Cuentan con controles de seguridad desactualizados para evitar ataques de virus o errores por parte del personal que afectan a la información, de tal manera que no garantizan su disponibilidad, integridad y confidencialidad. No realizan un adecuado análisis de riesgos, por lo que éstos y su impacto no son conocidos por lo cual no vienen tratándose, mucho menos se lleva un registro ni documentación de las incidencias.

Por lo mencionado anteriormente, es necesario y vital la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma Técnica Peruana SO/IEC27001 para proteger la información de la empresa Fiberlux S.A.C. y minimizar sus daños, de tal manera que se garantice la continuidad del negocio gracias a la implantación de controles actualizados, los cuales tienen que estar supervisados, revisados y actualizados en caso sea necesario; además, fortalecer la calidad de servicio que brinda, reduciendo posibles riesgos que le están afectando.

La presente investigación está enfocada a establecer si existe correlación entre la variable Sistema de Gestión de Seguridad de la Información y la variable calidad de servicio en la empresa Fiberlux S.A.C. y analizar el nivel de dicha relación.

1.2. Formulación del problema

1.2.1. Problema general.

¿Existe relación entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?

1.2.2. Problemas específicos.

1. ¿Existe relación entre la integridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?
2. ¿Existe relación entre la disponibilidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?
3. ¿Existe relación entre la confidencialidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?

1.3. Objetivos de la investigación

1.3.1. Objetivo general.

Determinar la relación que existe entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

1.3.2. Objetivos específicos.

1. Determinar la relación que existe entre la integridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.
2. Determinar la relación que existe entre la disponibilidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.
3. Determinar la relación que existe entre la confidencialidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

1.4. Justificación de la investigación

1.4.1. Justificación práctica.

De forma práctica, la presente investigación se justifica debido a que su resultado permitió determinar si existe una relación significativa entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, con lo cual dicha empresa gestiona los riesgos y así mejoró la calidad de servicio. Con los resultados de la investigación se propone cambios y recomendaciones para lograr mejorar la gestión de seguridad de la información.

1.4.2. Justificación teórica.

Con la presente investigación se tiene una justificación de forma teórica porque utiliza teorías y conceptos básicos de sistemas de gestión de seguridad de la información y sobre calidad de servicio para encontrar explicaciones a situaciones internas que venían afectando a la empresa Fiberlux S.A.C. en el 2023. Ello permitió al investigador comparar conceptos diferentes de las dos variables y sus respectivas dimensiones, además con esta investigación se genera nuevos aportes teóricos referentes a las variables del estudio, que servirán como bases teóricas en investigaciones futuras.

1.4.3. Justificación metodológica.

El presente trabajo de investigación se desarrolló mediante diseño no experimental, de tipo correlacional. Para alcanzar los objetivos de estudio, se empleó como técnica de investigación a la encuesta y como instrumento el cuestionario; su procesamiento se hizo a través de métodos estadísticos. Los resultados de la investigación se apoyan en técnicas de investigación que son válidas en el medio.

1.5. Delimitaciones del estudio

1.5.1. Delimitación espacial.

Este trabajo de investigación se desarrolló en la empresa Fiberlux S.A.C. en el 2023, la cual se encuentra ubicada en la av. José Pardo N°513, en el distrito de Miraflores, en la ciudad de Lima.

1.5.2. Delimitación social.

La presente investigación incluye a los trabajadores que utilizan información sensible dentro de la empresa Fiberlux S.A.C. en el 2023.

1.5.3. Delimitación temporal.

Esta investigación está referida a un tema de actualidad como es el sistema de gestión de seguridad de la información y la calidad de servicio, y se desarrolló entre los meses de noviembre y diciembre del 2023 para la recolección de información y desde enero a febrero del 2024 para el procesamiento de dicha información.

1.5.4. Delimitación conceptual.

Esta investigación abarca las diferentes teorías estudiadas, actualizadas y aplicadas durante los últimos años por diferentes autores, acerca de sistemas de gestión de seguridad de la información y calidad de servicio.

1.6. Viabilidad del estudio

El presente trabajo de investigación cuenta con el presupuesto auto financiado por el investigador por lo que es viable, existen fuentes teóricas que respaldan la presente investigación, cuenta con el apoyo de profesionales especializados en el tema de investigación, así como también de metodólogos, asesores temáticos y estadísticos.

Capítulo II. Marco teórico

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales.

Arias (2019) realizó un trabajo de investigación titulado “Plan de mejoramiento de la calidad del servicio y satisfacción de los usuarios del Gobierno Autónomo Descentralizado Municipal de Sucumbios por el periodo septiembre 2018 – febrero 2019” presentado a la Universidad Central del Ecuador, ubicada en Quito. Tuvo como objetivo principal proponer el plan de mejoramiento de la Calidad del Servicio y Satisfacción de los Usuarios del Gobierno Autónomo Descentralizado Municipal de Sucumbíos, a través de la aplicación de la norma ISO 9001-2015. El método de la investigación utilizado fue el deductivo, la muestra fue aleatoria, el instrumento para recolectar los datos aplicado fue un cuestionario. Concluyó con que el usuario del servicio en el del Gobierno Autónomo Descentralizado Municipal de Sucumbíos en general tiene la percepción que el servicio que se presta en esta gubernatura es insatisfactorio por muchos factores, con la investigación se ha determinado las posibles soluciones que se tienen a los problemas específicos cumpliendo el objetivo general del trabajo.

Bravo (2018), en su trabajo de investigación de maestría titulado “Desarrollo de un Sistema de gestión de seguridad de la información para bibliotecas basado en una metodología mejorada de análisis de riesgos compatible con la norma ISO/IEC 27001:2013”, presentada a la Escuela Politécnica Nacional, en Quito, Ecuador. Su objetivo principal fue fomentar la implementación de un Sistema de Gestión de Seguridad de la Información para bibliotecas basado en una metodología mejorada de análisis de riesgos mejorado para los activos y procesos de una biblioteca y que sea compatible con la norma ISO/IEC 27001:2013. Utilizó la metodología Action Research caracterizada por el aporte entre el investigador y los miembros

de la organización para solventar los problemas de la organización. Como conclusión indicó que, con que el sistema de gestión de seguridad de la información, se alcanzó identificar los activos no inventariados, amenazas y riesgos potenciales con lo que logró alcanzar la eficiencia en la gestión de los recursos de la organización además brindó mecanismos de protección y mejoramiento de sus recursos que se basan en un ciclo de mejora continua, lo que hará que la biblioteca alcance sus objetivos y fines propuestos.

Esguerra y Ortiz (2018) desarrollaron un trabajo de investigación titulado “Propuesta de implementación de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001:2013 para la empresa Lovato City Gas S.A.S” presentado a la Universidad Distrital Francisco de Caldas, Bogotá, Colombia. El objetivo principal fue brindar una propuesta de implementación para un sistema de gestión de la seguridad de la información (SGSI) que incluya estándares de seguridad basados en la norma ISO 27001: 2013, para los procesos de la empresa Lovato City Gas S.A.S. La investigación es de tipo aplicada, utilizó el ciclo PHVA y la metodología Magerit para realizar el análisis de riesgos, encontrando las amenazas y vulnerabilidades que presentaba la empresa. Entre los resultados se encontró la falta de políticas, objetivos, alcances y planes de tratamiento, que logren mantener los activos de información protegidos, por lo que concluye que era vital la implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001 de 2013, con el objeto de gestionar y mantener el control óptimo sobre la información y procesos que maneja la organización, donde se implementaron un conjunto de políticas de seguridad de la información las cuales optimizarán la protección, desempeño y efectividad de los procesos de la organización.

Guerra (2020), desarrolló un trabajo de investigación titulado “Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la biblioteca de la Universidad de la Costa”, en Barranquilla, Colombia. Su objetivo fue desarrollar un Sistema de Gestión de Seguridad de la Información, basado en la normativa ISO/IEC 27001:2013, esta normativa tiene como objetivo analizar, reducir el riesgo, mejorar y garantizar la seguridad de la información, estableciendo la estandarización de procesos en la biblioteca de la institución educativa superior Universidad de la Costa, el tipo de estudio es aplicada, retrospectiva, transversal, descriptivo y documental. Concluyó indicando que el sistema de gestión de seguridad de la información es importante dentro de la empresa porque logró identificar los riesgos asociados a cada proceso, así como conocer el nivel de su impacto para ser examinado, según las amenazas y vulnerabilidades, además se implementó controles para reducir o mitigar los riesgos para los procesos de calidad en la biblioteca de la Universidad de la Costa.

Olivera (2019) realizó un trabajo de investigación llamado “Procedimiento para implementar un sistema de seguridad de la información como contribución a la calidad de la información de los servicios de consultoría. Aplicación en el Ciget de Holguín” presentado a la Universidad de Holguín, Cuba. Dicho trabajo tiene como objetivo Desarrollar un procedimiento para implementar un sistema de gestión de seguridad de la información normalizado en el Ciget de Holguín que contribuya a mejorar la calidad de la información de los servicios de consultoría. Para la realización de esta investigación se aplicaron métodos teóricos y empíricos, como también técnicas y herramientas de la ingeniería industrial y otras especialidades afines. Entre los métodos teóricos se encuentran inductivo-deductivo que aportó a realizar generalizaciones y razonamientos luego de conocer las interioridades de la seguridad de la información, además de analizar el sistema en el diseño y aplicación del procedimiento

que se propusieron, se aplicaron técnicas como entrevistas a colaboradores y especialistas de información en el territorio, observación directa, entre otras. Concluyó con que, mediante el trabajo de investigación, se aportó en elevar la cultura de gestión de seguridad por parte de los colaboradores y determinar nuevas competencias de formación de los mismos; redefinir los roles y responsabilidades de seguridad; examinar la organización con relación a los requisitos de la Norma ISO/IEC 27001:2016 y del marco regulatorio asociado y poseer un inventario total de los activos de información de la empresa.

2.1.2. Antecedentes nacionales.

Elorrieta (2022) realizó una investigación titulada “Sistema de gestión de seguridad de la información y la calidad de servicio informático en la Universidad José Carlos Mariátegui, año 2019”, en la ciudad de Moquegua. Su objetivo fue determinar la relación entre el Sistema de Gestión de Seguridad de la Información (SGSI) y la calidad de los servicios de cómputo de la Universidad José Carlos Mariátegui, Año 2019. Es una investigación aplicada, de diseño no experimental, de nivel correlacional y de tipo transversal. Como conclusión, se demostró que existe una relación entre el Sistema de Gestión de Seguridad de la Información (SGSI) y la Calidad del Servicio de tecnología de información, lo que logró saber la situación actual en el proceso de seguridad de la Universidad José Carlos Mariátegui, año 2019, lo que le ayuda a aumentar su rendimiento garantizando la seguridad, confiabilidad y disponibilidad de la información.

Pacheco (2021) realizó un trabajo de investigación titulado “Implementación de un sistema de gestión de calidad aplicando la norma ISO 9001:2015 ISO-IEC para mejorar la gestión administrativa de la Empresa Naylamp Ingenieros S.A.C.”, presentado a la Universidad Continental, en Lima. Tuvo como objetivo principal implementar el Sistema de Gestión de la

Calidad aplicando la Norma ISO 9001:2015 para mejorar la gestión administrativa de la empresa Naylamp Ingenieros S.A.C. Es una investigación de tipo aplicada porque el objetivo es aplicar el saber existente en la solución de un problema práctico, es de diseño no experimental, de nivel correlacional. Concluye con que, gracias a la implementación del sistema de gestión de calidad aplicando la Norma ISO 9001:2015, se mejora la gestión administrativa de la empresa Naylamp Ingenieros S.A.C., esto se evidencia en el incremento del porcentaje (26%) de conocimiento y aplicación de la norma en sus actividades diarias con respecto a la medición realizada en el diagnóstico inicial.

Sánchez (2023) realizó la tesis llamada “Seguridad de la información y calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión”, en la ciudad de Huacho. El objetivo principal fue determinar la relación entre la seguridad de la información y la calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión. La investigación es de tipo aplicada, de diseño no experimental, de nivel correlacional, de corte transversal. Se concluye con que la seguridad de la información posee una alta correlación (0,881) con la calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión. La relación indica que la media de puntaje logrado en la seguridad de la información es de 3,82, sobre el puntaje máximo que es de 5, lo que en su escala valorativa equivale a “regular” con tendencia a ser “Bueno”, y la media de calidad de servicio es de 4,07 que en su escala valorativa es igual a bueno, lo que quiere decir que hay una relación directa, es decir, existe una confiabilidad de la información con una calificación de regular con tendencia a ser bueno y una calidad de servicio de nivel bueno.

Vergara (2017), en su trabajo de investigación titulado “Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016” desarrollado en la

ciudad de Lima. Tuvo como objetivo determinar la relación entre la seguridad de información y la calidad de servicio en la Universidad Nacional Federico Villarreal en el año 2016. La investigación utilizó el método hipotético deductivo con enfoque cualitativo, de diseño no experimental, de nivel correlacional, de corte transversal. Concluye con que se ha establecido que existe una relación directa y significativa de nivel moderado entre la seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016, obteniendo como resultado Rho de Spearman = 0.683** y un p-valor =0.000<0.05, quedando comprobada la hipótesis alterna y se rechaza la hipótesis nula.

Zarbe (2019) desarrolló una tesis llamada “Sistema de gestión de seguridad de la información para la calidad de procesos en la I.E.P. Albert Einstein”, presentada a la Universidad Nacional de Ucayali, en la ciudad de Pucallpa. Tuvo como objetivo establecer el desarrollo de un sistema de gestión de seguridad de información en la calidad de procesos para la I.E.P. Albert Einstein. La investigación es de tipo aplicada debido a que la implementación de un Sistema de Gestión de Seguridad de la Información realiza una solución para el problema de la I.E.P. Albert Einstein; es de diseño no experimental, de nivel correlacional, contando con una población de 8 trabajadores. Concluyó con que se mejoró en un 60% la seguridad de la información y los activos de la información en la I.E.P. Albert Einstein, a través de la propuesta de desarrollo de un Sistema de Gestión de Seguridad de la Información.

2.2. Bases teóricas

2.2.1. Sistema de gestión de seguridad de la información (X).

Olivera (2019) en su investigación lo define como un conjunto de elementos que se encuentran relacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que emplea una

organización para implementar sus políticas y unos fines de seguridad de la información y poder lograr alcanzar dichos objetivos, a través de un enfoque de gestión y de mejora continua.

Ccesa (2017) en su trabajo de investigación lo define como el conjunto de procesos que establecen, implementan, mantienen y mejoran de forma continua la seguridad de la información, basándose en los riesgos a los que se vienen enfrentando la organización. También mencionan que la implementación de un SGSI incluye el establecimiento de procesos formales y un claro establecimiento de responsabilidades basándose en una serie de políticas, planes y procedimientos que deberán estar documentadas.

De acuerdo a Castro (2018), el sistema de gestión de seguridad de la información es un conjunto de elementos relacionados o que tienen interacción en cuanto a estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos empleados por una empresa para determinar políticas y objetivos de la seguridad de la información. También indica que la implementación de un sistema de gestión de la seguridad de la información se basa en la norma ISO 27001, utilizando el ciclo Deming el cual permite implantar un plan de mejora continua. El ciclo Deming tiene las siguientes etapas:

Planificar: Castro (2018) indica que en esta etapa se establece el alcance y la política de seguridad, empezando con un análisis de riesgo para conocer la situación actual de la organización, establece un plan de tratamiento de información y de riesgos, para seguir con la implementación de controles para los diferentes riesgos que la gestión no está tomando en cuenta.

Hacer: Castro (2018) indica que en esta etapa del ciclo Deming o ciclo PDCA se focaliza en la planificación de los tratamientos de riesgos, esto abarca la concientización de los usuarios, y la definición de medidas para los distintos controles que se van a implementar.

Verificar: Castro (2018) indica que en esta etapa abarca la realización de auditorías para examinar la correcta implementación del sistema de gestión de la seguridad de la información, la realización de auditorías internas y la gestión general de la organización.

Actuar: Castro (2018) indica que en esta etapa se revisa el resultado de la auditoria y se toman diferentes acciones correctivas, preventivas o de mejora.

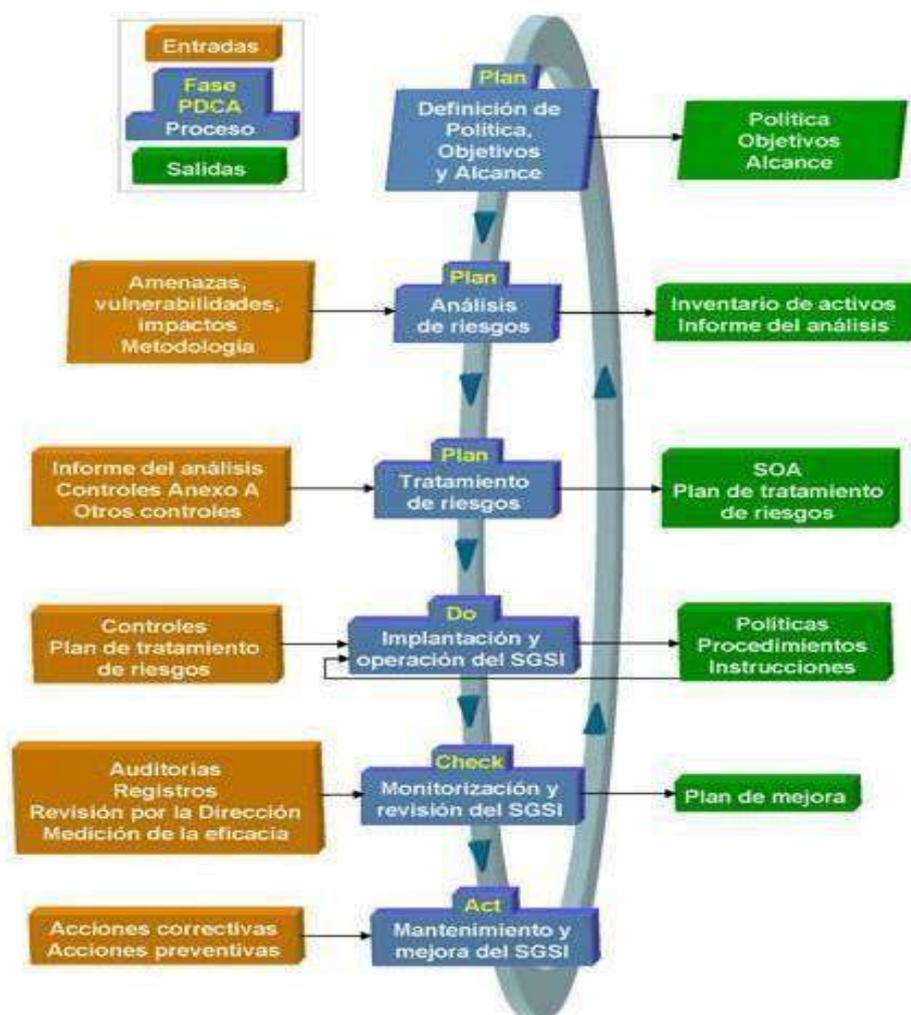


Figura 1. Ciclo de Deming

Fuente: ISO 27000

Para Torres (2018), “el sistema de gestión de seguridad de la información recoge un conjunto de procedimientos y políticas que tienen como objetivo conseguir y preservar los principios básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad) ya comentados previamente” (p.67).

Según Trujillo (2020), el sistema de gestión de seguridad de la información proporciona diferentes procesos y herramientas basados en la norma ISO27001, la cual favorece a diferentes organizaciones o entidades en la identificación de las debilidades referentes a la seguridad de la información, dirigiendo al usuario para una eficaz gestión de los riesgos.

2.2.1.1. Seguridad de la información.

Olivera (2019) la define como “un proceso integrado por estrategias, medidas preventivas y medidas reactivas que se ponen en práctica en las instituciones para proteger la información y mantener su confidencialidad, disponibilidad e integridad de la misma” (p.5-6).

Godoy (2014) en su trabajo de investigación indica que la Seguridad de la Información tiene como fin proteger la información y los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizadas. La seguridad se entiende como un estado de cualquier sistema o tipo de información (informático o no) que nos demuestra que ese sistema o información está libre de cualquier peligro, daño o riesgo. El peligro o daño es todo aquello que puede afectar a su funcionamiento directo o a los resultados que se logran obtener. También se contempla que la seguridad de la información es un conjunto de medidas preventivas y reactivas de las empresas y de los sistemas tecnológicos que logran resguardar y proteger la información mediante el mantenimiento de la confidencialidad, la disponibilidad e integridad de la misma.

Según, la Norma ISO 27001 (2013), la seguridad de información, protege a la información de una serie amplia de amenazas, con el objeto de garantizar la continuidad del negocio, reduciendo el daño del mismo y maximizando el retorno de las inversiones y nuevas posibilidades. Además, abarca la existencia de la información en varias formas como; impresa o escrita en papel, en forma electrónica, transmitida por un medio electrónico, presentada en imágenes, o expuesta en una conversación. Cualquiera que sea la manera como se encuentre la información, o los medios mediante los cuales se distribuye o centraliza (almacenamiento), se debe proteger y resguardar siempre de una forma óptima que permita preservar la confidencialidad, integridad y disponibilidad, términos que conforman la base de la seguridad de la información. Para lograr que la seguridad de la información sea gestionada correctamente, se utiliza un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información.

2.2.1.2. Ventajas de la ISO/IEC 27001:2016.

De acuerdo a la NC ISO/IEC 27001:2016 (2016), las organizaciones mejoran su rendimiento debido a las siguientes ventajas:

- Es una norma con reconocimiento internacional.
- Eficiencia en la gestión de la empresa: Al tomarse medidas para minimizar los riesgos que se asocien a la gestión de la información.
- Solvencia empresarial: Por disponer de un sistema que garantiza la confidencialidad, integridad y disponibilidad de la información.
- Continuidad: Como consecuencia de la implantación de planes de continuidad de negocio que evitan paradas no deseadas de la actividad empresarial.

- Mejora de la imagen de la empresa: Al evidenciar su compromiso con la seguridad de la información propia y de clientes.

2.2.1.3. Gestión del riesgo.

Zarbe (2019) define a la gestión del riesgo como una mezcla entre las actitudes de los interesados ante al riesgo y la exposición al riesgo estratégico de un proceso, haciendo un análisis del perfil de riesgo de los interesados para clasificar y calificar el apetito y la tolerancia al riesgo de los interesados del proyecto. La gestión de riesgo es un enfoque estructurado para el estudio de la posibilidad de que suceda o no un riesgo, por lo que, para que no ocurra el riesgo, se realizan actividades para examinar, reducir el riesgo y estrategias para su manejo, reducirlos o aceptarlos, de manera que las posibles pérdidas y la posibilidad que se haga presente el riesgo se reduzcan. En conclusión, la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para después implementar mecanismos que permitan controlarlo.

Arévalo, Cedillo y Moscoso (2017) afirman que “la gestión de riesgos se define como una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida para la organización” (p.31).

Osorio (2016) contempla que la administración del riesgo consiste en poder hacer pronósticos e identificar las diferentes acciones o circunstancias que podrían alterar aspectos estratégicos, financieros, sociales y legales de cualquier empresa, considera también que para hacer una óptima gestión de riesgos es importante que cada miembro de la organización sea consciente de los riesgos a los que se enfrentan diariamente y de esa manera, sean más responsables en proteger los activos.

2.2.1.4. Dimensiones de Sistemas de gestión de seguridad de la información.

2.2.1.4.1. Integridad de la información (X1).

Méndez (2021) señala que “integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas; es decir, que los datos sean exactamente fueron creados sin alteraciones ni manipulaciones por parte de terceros” (p.20).

Godoy (2014) la define como la propiedad que trata de mantener los datos libres de alteraciones no autorizadas, la integridad es mantener con exactitud la información tal como fue generada, sin ser manipulada o modificada por personas o procesos sin autorización.

Vergara (2017) agrega que la integridad quiere garantizar que no se hagan alteraciones por individuos sin autorización al acceso de los datos o procesos, que no se hagan manipulaciones no autorizadas por personal autorizado a los datos o procesos y que los datos se mantengan consistentes tanto interna como externamente.

Esguerra y Ortiz (2018) afirman:

Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizadas o accidentales. (p.18)

Según Narro (2021):

La integridad evita que la información que maneja y transita por toda la organización sufra modificaciones o errores, para la presente investigación con la integridad se busca evitar la alteración intencionada o errores involuntarios, y así evitar la toma de decisiones basadas en información equivocada que puede generar pérdidas económicas, vulneración de información privada (datos de estudiantes y trabajadores), entre otros; colocando en riesgo la continuidad del propósito de la organización. (p.16)

Sandoval (2021) agrega sobre integridad:

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben de asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información. (p.21)

2.2.1.4.2. Disponibilidad de la información (X2).

Godoy (2014) en su trabajo de investigación la define como la propiedad cualidad o condición de la información de permanecer a disposición de quienes deben acceder a ella, sean personas, procesos o aplicaciones, la disponibilidad es el acceso que se tiene a la información y a los sistemas por parte de personal autorizado en el momento que así lo necesiten.

Esguerra y Ortiz (2018) afirman sobre disponibilidad “se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad implica pérdida de productividad de la entidad” (p.18).

Según Olivera (2019) “la integridad protege la información y los sistemas para que no sean modificados por personas no autorizadas; asegura que los datos sean precisos y confiables” (p.9).

Méndez (2021) señala que “la información puede ser accedida en el momento que sea requerida a través de canales adecuados siguiendo los procesos correctos” (p.21).

Narro (2021) afirma que la disponibilidad logra acceder a la información cuando se requiera en cualquier momento del día, mes o año; para su investigación fue necesario mantener acceso al correo institucional en todo momento, porque mediante él funciona el trámite documentario interno y externo, así como la administración educativa para el acceso al sistema académico, la carencia de disponibilidad en cualquier organización generaría la paralización parcial o total de las actividades.

Sandoval (2021) agrega sobre disponibilidad, está referido a la continuidad de acceso a los diferentes elementos de información almacenados y procesados en un sistema informático. Según esta característica, las herramientas de seguridad informática deben de fortalecer el mantenimiento del sistema informático, en condiciones adecuadas para lograr que los usuarios accedan a los datos con la frecuencia y dedicación que ellos requieran, esta característica es importante en sistemas informáticos cuyos compromisos con el usuario, es prestar servicio de forma constante. La seguridad informática se encarga de que la información manejada por un

computador no sea dañada o alterada, es decir, cuidar su integridad, que esté disponible y en condiciones que permita su procesamiento en cualquier momento y se mantenga de forma confidencial.

Vergara (2017) indica que “la disponibilidad, asegura que los usuarios autorizados tienen el acceso adecuado a la información” (p.37).

2.2.1.4.3. Confidencialidad de la información (X3).

Olivera (2019) la define como “propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información” (p.8).

Godoy (2014) agrega que es “la propiedad que imposibilita la divulgación de información a personas o sistemas no autorizados, asegurando únicamente a aquellas personas que cuenten con la debida autorización para el acceso a la información” (p.165).

Esguerra y Ortiz (2018) indican sobre confidencialidad “se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede terminar en problemas legales, pérdida del negocio o credibilidad” (p.18).

Narro (2021) sostuvo que la confidencialidad tiene por objetivo que la información se encuentre accesible sólo al personal autorizado en los diversos niveles que existan en la organización (personas, entidades o sistemas); la confidencialidad busca que no exista el robo total o parcial de información sensible ya sea por parte del propio personal o de algún ataque a través de internet y sobre todo tratar de que no exista la divulgación o uso no adecuado de esta información.

Sandoval (2021) agrega sobre confidencialidad que esta referida a la privacidad de la información almacenada y procesada en un sistema informático, es decir, las herramientas de seguridad informática tienen que proteger el sistema de posibles ataques y accesos por parte de intrusos o programas no autorizados. La confidencialidad es importante en sistemas distribuidos, es decir aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente conectados.

Vergara (2017) afirma que la confidencialidad tiene por objetivo la prevención al acceso no autorizado a la información, ya sea que fuera intencional o no intencional. La pérdida de la confidencialidad puede presentarse de varias maneras, como por ejemplo con la publicación intencional de información confidencial de la empresa.

2.2.2. Calidad de servicio (Y).

Bravo (2021) la define como una estrategia competitiva y diferencial que está asociada con los procesos de compra y venta, mediante un conjunto de acciones que pretenden mejorar la experiencia entre el consumidor y la marca, y construir relaciones durables entre ambos. Para lo cual, deben crear un ambiente que sea positivo, servicial y amigable que garantice buenas percepciones al cliente e incluso sobrepase sus expectativas.

Bravo (2021) también agrega “calidad de servicio es la situación en la cual, una empresa otorga calidad y servicios superiores a sus clientes, propietarios y empleados. Significa que todas las características, actos e información deben aumentar la capacidad de producir valor para el cliente” (p.30).

Maquera (2022) afirma que “calidad de servicio es la conformidad de los usuarios receptores y realidad en la percepción, lo que los usuarios deseen es la preservación de la información mediante las dimensiones tangibilidad, confiabilidad, tiempo de respuesta, seguridad y empatía” (p.17).

Cacuango (2019) indicó la siguiente definición:

Es el rendimiento de los servicios que determinan un nivel de satisfacción de los usuarios de dicho servicio. QoS también se define como un conjunto de tecnologías que permiten a los administradores de red manejar los efectos de la congestión del tráfico usando óptimamente los diferentes recursos de la red. La calidad de servicio en una red permite administrar y controlar parámetros de algunos tipos de tráfico como audio, video y datos digitales (software, documentos, base de datos y archivos), además controla los flujos de tráfico que producen diferentes servicios al cruzar por la red que se comunican y así poder entregar correctamente la información al usuario sin pérdida de datos. (p.19)

Vergara (2017) la define como:

Es la percepción del servicio esperado por el cliente, el cual se mide por el nivel en que el cliente desea percibir y satisfacer sus necesidades. El uso del producto efectivo se origina en la capacidad para su medida, también se define como el grado en el que se han cumplido los requisitos del cliente quedando claro que aun si el cliente ha pactado sus requisitos con la empresa u organización, la satisfacción elevada no está asegurada por el cliente; de la misma forma señalar que la calidad se encuentra asociada a un bien o servicio, que sin que haya tenido una experiencia del servicio o consumo el cliente, surge la imagen y reputación de la empresa, por

lo tanto los reclamos de los usuarios son considerados como indicadores de satisfacción baja, a su vez el ausentamiento de los mismos no siempre debe ser considerada como la satisfacción de alto nivel. (p.40)

Vergara (2017) dentro de su trabajo de investigación agrega lo siguiente:

La calidad de servicio es proveniente de la contigüidad entre el servicio deseado y el servicio percibido, mide el nivel percibido por el cliente, sobre las exigencias deseadas por él mismo, después de idearse una opinión sobre servicio recibido. Ésta es la forma de medir la capacidad para su uso del bien inherente a la definición de calidad establecido por Juran. También es una forma de medir las exigencias del cliente. Inclusive cuando las exigencias del cliente hayan sido entabladas con la organización y que se haya cumplido con dicho pacto, no se asegura la satisfacción del cliente. Del mismo modo, consideran que la apreciación de calidad en relación a un producto, puede surgir inclusive sin que el cliente haya experimentado el consumo del mismo, originándose del prestigio e imagen organizacional. (p.39-40)

2.2.2.1. Parámetros de calidad de servicio.

Cacuango (2019) en su trabajo de investigación señala:

Los parámetros de calidad de servicio son instrumentos de medición; de carácter tangible y cuantificable, que permiten evaluar la calidad de los procesos, productos y servicios para asegurar la satisfacción de los clientes; es decir, miden el nivel de cumplimiento de las especificaciones establecidas para una determinada actividad o proceso empresarial. La calidad de servicio al ser usada correctamente ayuda a prevenir la congestión de la red, seleccionando el tráfico de acuerdo a su prioridad, y utilizando métodos de control. (p.19)

En su investigación Cacuango (2019) lista una serie de parámetros que se deben utilizar para la calidad de servicio, los cuales son:

Jitter: es la variabilidad del tiempo de ejecución de los paquetes en la cual los paquetes llegan demasiado pronto o tarde para poder ser entregados.

Latencia: Lapso de tiempo en que un paquete va de su origen al destino, este parámetro es muy importante en el cual se debe tener el menor retardo posible en las comunicaciones.

Rendimiento: Es la capacidad que tiene un enlace para transportar información útil este parámetro se define por el tiempo que tiene desde la salida y llegada del paquete de la información.

Perdida de paquetes: cuando un paquete enviado llega tarde a su destino, algunos paquetes que son enviados a través de protocolos UDP van sin seguridad por lo que no llegarán a su destino y no serán reenviados para alcanzar su destino (Cacuango, 2019).

2.2.2.2. Características y propiedades de la calidad de servicio.

En su trabajo de investigación, Vergara (2017, p.41) señala las siguientes:

Los servicios son intangibles, es decir no se pueden palpar.

Los servicios son prestados por única vez.

El servicio se realiza y consume simultáneamente.

La prestación del servicio, en el cliente juega un papel primordial.

Un servicio prestado, no se puede corregir.

Hay que planificar la realización del servicio con anticipación, para garantizar la calidad del servicio.

Es necesario establecer responsabilidades específicas para complacer las exigencias e intereses del usuario (cliente).

El servicio prestado es personal, quiere decir que la calidad está casi determinada.

La estandarización del servicio es compleja, por lo que perdura la posibilidad de cometer errores.

El servicio es caracterizado por que realiza transacciones directas.

En la prestación interactúan múltiples procesos.

En el momento de la prestación del servicio, se suscita una retroalimentación con el cliente.

El servicio prestado (intangibles), en oportunidades está relacionado a un producto.

El servicio prestado inadecuadamente, determina generalmente la pérdida del cliente.

2.2.2.3. Factores de la calidad de servicio.

Vergara (2019, p.41) indica los siguientes factores:

La eficacia de la organización en la administración de las expectativas de los clientes.

El conocimiento de los productos de la competencia y de la misma organización por parte de los clientes.

El método de las comunicaciones que utiliza la organización.

Las consideraciones de terceros respecto a la organización.

2.2.2.4. Dimensiones de calidad de servicio.

2.2.2.4.1. Fiabilidad (Y1).

Vergara (2017) afirma que “la fiabilidad es una destreza para realizar la prestación prometida de manera confiable. La fiabilidad, es entendida como la capacidad de cumplir bien a la primera con los compromisos adquiridos” (p.46).

Retuerto (2017) sostiene que fiabilidad:

Se entiende como la habilidad de desarrollar el servicio prometido precisamente en la forma pactada y con exactitud. Resulta sencillo entender la importancia de esta dimensión para un cliente potencial, por lo que la organización, debe prestarle atención para poder satisfacer esta exigencia, antes de realizar el propio servicio. El encontrar y definir apropiadamente los procedimientos que permitan cumplir con esta exigencia, permitirá a la organización alcanzar el tan anhelado objetivo de poder brindar un servicio de calidad, pues si mínimamente no se puede cumplir con ello, el cliente no percibirá el servicio como bueno. (p.36)

Arias (2019) afirma lo siguiente:

El servicio debe prestarse de manera eficiente y correcta desde el comienzo; porque aquí es donde está la habilidad de brindar un excelente servicio observándose de manera segura, fiable y cautelosa. Esto se divide en seguir con las pautas establecidas, realizar bien las labores de trabajo desde el principio; y el servicio debe ejecutarse en el tiempo disponible y especificado. (p.20)

2.2.2.4.2. *Capacidad de respuesta (Y2).*

Arias (2019) indica la siguiente definición “la disposición que tiene la empresa para ofrecer respuestas de manera oportuna y ágil a los usuarios, esto debe proporcionarse de manera eficiente y rápida, la finalidad es que siempre debe superar las expectativas estipuladas” (p.20).

Vergara (2017) sostiene que es “la capacidad de respuesta es la atención demostrada y la disposición positiva de los colaboradores, asimismo, las habilidades para inspirar credibilidad y confianza ante los usuarios (clientes). La capacidad de respuesta determina poder ofrecer un servicio al cliente con rapidez” (p.46).

Retuerto (2017) afirma que:

La capacidad de respuesta está directamente relacionada, no solo con la velocidad de respuesta, sino con la propia habilidad que tienen los trabajadores para resolver situaciones o inconvenientes que puedan presentarse en la jornada de trabajo. De ahí la importancia en las capacitaciones o preocupaciones de la dirección de la organización en fomentar un ambiente laboral cómodo y satisfactorio para que el trabajador, pueda realizar su trabajo con la mejor disposición, mejorando la imagen global del servicio. (p.38)

2.2.2.4.3. *Tangibilidad (Y3).*

Vergara (2017) considera la siguiente definición “es el aspecto exterior de las instalaciones, maquinas, personal y equipos de comunicación” (p.45).

Además, Vergara (2017) agrega que “la tangibilidad está compuesta por elementos tales como la apariencia de las instalaciones físicas, el mantenimiento y modernidad de los equipos, el aspecto de los materiales de comunicación y la apariencia física de las personas” (p.45).

Retuerto (2017) afirma que:

Está relacionada con la presencia de las instalaciones físicas, equipo, personal, etc. Se refiere a aspectos físicos que el cliente percibe en la organización, podemos resumir este concepto, como aquello que puede ser percibido por nuestros sentidos. Elementos como limpieza o modernidad son examinadas en los elementos personas, infraestructura y objetos. (p.37)

2.3. Definiciones de términos básicos

Activo

Esguerra y Ortiz (2018) lo definen como “es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.” (p.22-23).

Amenaza informática

Esguerra y Ortiz (2018) la definen como “la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información” (p.20).

Análisis de riesgo

Sandoval (2017) afirma “es el estudio de las posibles amenazas y probables eventos no deseados es decir los daños y consecuencias que éstas puedan producir” (p.32).

Ataque

Cáceda (2021) afirma “es el intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada” (p.17).

Control

Cáceda (2021) indica “medio de la gestión de riesgos, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter jurídico. También se utiliza como sinónimo de salvaguardia o de contramedida” (p.17).

Eficiencia

Trinidad (2019) señala que se da “cuando se logran los objetivos planificados en la organización, utilizando el menor costo posible y en el mínimo tiempo, sin gastar recursos y con el máximo nivel de calidad factible” (p.53).

Eficacia

Trinidad (2019) afirma “capacidad de alcanzar el efecto que se espera. Además, contenido de una empresa para lograr los objetivos trazados, obtener los resultados deseables, realizando las cosas correctamente” (p.53).

Impacto

Narro (2021) indica “es considerado como el impacto del daño causado cuando una amenaza se materializa sobre un activo, ese impacto se suele calcular en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo (p.29).

Información

Trinidad (2019) sostiene “por información nos referimos al conjunto integral de datos con un específico significado” (p.53).

ISO 27001

Esguerra y Ortiz (2018) indican “es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa” (p.18).

Política de calidad

Pacheco (2021) la define como “directivas e intenciones generales de una organización relacionadas con la calidad, tal cual son oficialmente formuladas por la dirección” (p.31).

Riesgo

Pacheco (2021) lo define como “probabilidad de que algo desagradable acontezca, afectando el correcto desempeño de una actividad” (p.31).

Riesgo informático

Esguerra y Ortiz (2018) lo define como “incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos, como equipos informáticos, periféricos, instalaciones, programas de cómputo, etc.” (p.21).

Sistema

Bravo (2021) lo define como “conjunto de elementos interdependientes e interactuantes que forman un todo organizado para alcanzar un objetivo” (p.39).

Vulnerabilidad informática

Esguerra y Ortiz (2018) la definen como:

Posibilidades del mismo ambiente, en el cual las características se vuelven susceptible a una potencial amenaza, por lo que, se puede definir como la capacidad de reaccionar ante la presencia de una amenaza o un daño. Se es vulnerable a cualquier incidente, sin importar su naturaleza, sea esta interna o externa, pero aplicando los controles óptimos es posible reducir las

posibilidades de que estas se vuelvan realidad, por lo tanto, los tipos de vulnerabilidades. (p. 18)

2.4. Formulación de las hipótesis

2.4.1. Hipótesis general.

El sistema de gestión de seguridad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

2.4.2. Hipótesis específica.

1. La integridad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

2. La disponibilidad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

La confidencialidad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

2.5. Operacionalización de las variables

Variable 1: Sistema de gestión de seguridad de la información

Definición Conceptual:

Olivera (2019) lo define como un conjunto de elementos que se encuentran relacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que emplea una organización para implementar sus políticas y unos fines de seguridad de la información y poder lograr alcanzar dichos objetivos, a través de un enfoque de gestión y de mejora continua.

Definición operacional:

Dimensiones: Integridad de la información, disponibilidad de la información, confidencialidad de la información.

Variable 2: Calidad de servicio**Definición Conceptual:**

Bravo (2021) la define como una estrategia competitiva y diferencial que está asociada con los procesos de compra y venta, mediante un conjunto de acciones que pretenden mejorar la experiencia entre el consumidor y la marca, y construir relaciones durables entre ambos. Para lo cual, deben crear un ambiente que sea positivo, servicial y amigable que garantice buenas percepciones al cliente e incluso sobrepase sus expectativas.

Definición operacional:

Dimensiones: Fiabilidad, capacidad de respuesta, tangibilidad.

Tabla 1

Operacionalización de las variables

VARIABLES	DIMENSIONES	INDICADORES	ESCALA
Sistema de gestión de seguridad de la información (X)	X.1.- Integridad de la información.	X.1.1.- Seguridad de la comunicación. X.1.2.- Gestión de incidentes. X.1.3.- Seguridad lógica.	Escala de valoración Likert: 1 = Muy en desacuerdo
	X.2.- Disponibilidad de la información.	X.2.1.- Acceso a la información en el tiempo requerido. X.2.2.- Continuidad del negocio. X.2.3.- Procedimientos de respaldo.	2 = Algo en desacuerdo 3 = Ni de acuerdo ni en desacuerdo
	X.3.- Confidencialidad de la información.	X.3.1.- Privacidad de la información. X.3.2.- Autenticación. X.3.3.- Autorización.	4 = Algo de acuerdo 5 = Muy de acuerdo
Calidad de servicio (Y)	Y.1.- Fiabilidad.	Y.1.1.- Eficiencia. Y.1.2.- Eficacia.	Escala de valoración Likert: 1 = Muy en desacuerdo
	Y.2.- Capacidad de respuesta.	Y.2.1.- Tiempo de respuesta. Y.2.2.- Mejora continua.	2 = Algo en desacuerdo 3 = Ni de acuerdo ni en desacuerdo
	Y.3.- Tangibilidad.	Y.3.1.- Infraestructura. Y.3.2.- Condiciones generales. Y.3.3.- Almacenamiento.	4 = Algo de acuerdo 5 = Muy de acuerdo

Fuente: Elaborado por los autores.

Capítulo III. Metodología

3.1. Diseño metodológico

3.1.1. Método de la investigación.

Para el desarrollo de la investigación se aplicó el método Deductivo, debido a que el autor inició de aspectos generales en la investigación para poder encontrar situaciones particulares dentro de la empresa Fiberlux S.A.C.

3.1.2. Diseño de la investigación.

El autor ha considerado el diseño es No Experimental porque él no intervino ni manipuló ninguna de las dos variables, además valoró el comportamiento de las variables para establecer si existe correlación entre las mismas.

La investigación es de tipo Transversal o transaccional debido a que se comprendió el estado actual que presentaba una población determinada, por lo que la recolección de los datos de la población se realizó en un solo momento determinado durante el año 2023.

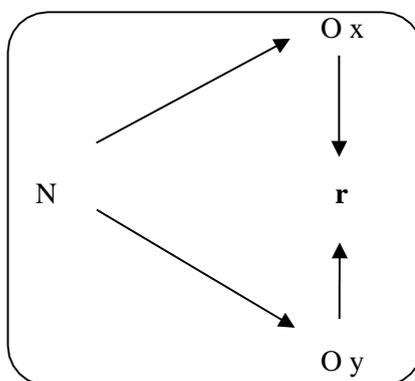
3.1.3. Tipo de Investigación.

La investigación es de tipo Aplicada porque está orientada a problemas actuales, concretos e identificables de la empresa Fiberlux S.A.C. a los que se les pudo aplicar soluciones actuales.

Este tipo de investigación tiene como punto de inicio el conocimiento generado por la investigación básica y del marco teórico definido que permite identificar problemas sobre los que se debe actuar como para definir las estrategias de solución.

3.1.4. Nivel de Investigación.

El nivel de investigación que se aplicó fue el Correlacional, para medir el grado de asociación entre las variables presentes, es decir se pretendió demostrar la relación que existe entre el Sistema de gestión de seguridad de la información y la calidad de servicio la empresa Fiberlux S.A.C. en el 2023, a través de las encuestas que se realizaron a los trabajadores de dicha empresa. La relación que existe entre las variables identificadas la podemos ver en la siguiente figura:



Denotación:

N = Población

Ox = Observación a la variable x.

Oy = Observación a la variable y.

r = Relación entre variables.

3.2. Población y muestra

3.2.1. Población.

En la presente investigación se consideró como población objetivo a los 55 trabajadores quienes vienen laborando en la sede del distrito de Miraflores, en la ciudad de Lima de la empresa Fiberlux S.A.C. en el 2023, quienes son los que están involucrados directamente con

el sistema de gestión de seguridad de la información y con los procedimientos relacionados con la calidad del servicio.

3.2.2. Muestra.

Para calcular el tamaño de la muestra, se utilizó la técnica de muestreo probabilístico, en la que hay que tomar en cuenta tres factores:

- El porcentaje de confianza con el cual se quiere generalizar los datos desde la muestra hacia la población total.
- El porcentaje de error que se pretende aceptar al momento de hacer la generalización.
- El nivel de variabilidad que se calcula para comprobar la hipótesis.

Una vez que se han determinado estos tres factores, entonces se puede calcular el tamaño de la muestra como a continuación se expone.

Tabla 2

Factores para el cálculo de la muestra

n =	Tamaño de la muestra
N =	Población total = 55
e =	Error de muestreo (5%)
z =	Porcentaje de fiabilidad (95%=1,96)
q =	Probabilidad de no ocurrencia (50%)
p =	Probabilidad de ocurrencia (50%)

Fuente: Elaboración propia

Aplicamos la siguiente fórmula:

$$n = \frac{z^2 Npq}{e^2(N - 1) + z^2 pq}$$

$$n = \frac{(1,96)^2 \times 55 \times 0,5 \times 0,5}{0,05^2 \times (55 - 1) + (1,96)^2 \times 0,5 \times 0,5}$$

n = 49 trabajadores

El tamaño de la muestra que se obtuvo fue de 49 trabajadores, la que representa el 89% de la población, siendo una muestra representativa.

3.3. Técnicas e instrumentos para la recolección de datos

3.3.1. Técnicas

La técnica que se empleó fue la encuesta, la cual estará orientada a la recolección de datos los cuales serán proporcionados por los trabajadores de la sede del distrito de Miraflores de la empresa Fiberlux S.A.C.

3.3.2. Instrumentos

El instrumento que se empleó en la recolección de la información, fue el cuestionario de encuestas, porque es un instrumento que sirve para recoger los datos que nos proporcionaron

los trabajadores de la empresa Fiberlux S.A.C. a través de un grupo de preguntas que constituyen el tema de la encuesta. Utilizamos el cuestionario simple con preguntas de opción múltiple con escala de calificación de 5 alternativas, para lo cual se utilizó la escala de Likert.

El cuestionario de encuestas fue sometido a validez de contenido mediante la técnica del juicio de expertos, para confirmar que el instrumento es válido y confiable.

3.3.2.1 Validación del Instrumento.

Para la validación del instrumento que se aplicó para la recolección de datos, se hizo mediante el juicio de experto, los cuales dieron la puntuación mostrada en la tabla:

Tabla 3

Juicio de expertos para el instrumento

Expertos	Grado	Puntuación
Ing. Jorge Martín Figueroa Revilla	Doctor	89,0
Ing. Juan José Flores Cueto	Doctor	88,5
Ing. Wigberto Martín Nicho Virú	Maestro	88,5
Promedio general		88,7%

Fuente: Elaboración propia.

Luego que se promediaron los puntajes dado por cada uno de los expertos, obtuvimos un puntaje de 88,7% para el instrumento, lo que indica que está en el rango de “Excelente”, demostrando así que el instrumento de esta investigación tiene una alta valoración brindada por expertos profesionales con conocimientos en instrumentos de recolección de datos.

3.3.2.2 Confiabilidad del Instrumento.

Para la comprobación de la Confiabilidad del instrumento ya validado se procedió a realizar una prueba piloto a 10 trabajadores de otra empresa quienes presentan características iguales a los sujetos considerados en la muestra. El procesamiento de las respuestas de la encuesta se hizo con el software SPSS Versión 26, luego del cual obtuvimos los resultados siguientes:

Tabla 4
Resumen del procesamiento de los casos del instrumento

		N	%
Casos	Válidos	10	100,0
	Excluidos	0	,0
	Total	10	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.
Fuente: Elaboración propia.

Tabla 5
Estadísticos de fiabilidad del instrumento

Alfa de Cronbach	N de elementos
0,90	10

Fuente: Elaboración propia.

Aplicamos el modelo estadístico Alpha de Cronbach, con el que logramos una confiabilidad de 0,90 para el instrumento, lo que quiere decir que tiene un nivel elevado de confiabilidad. La aplicación del análisis de Confiabilidad es un modelo estadístico de los más rigurosos para este tipo de pruebas.

3.4. Técnicas para el procedimiento de la información

3.4.1. Análisis documental

A través del análisis documental y sus respectivos instrumentos se revisaron fuentes bibliográficas, revistas, publicaciones especializadas y portales de Internet relacionados con el tema de la investigación.

Mediante la entrevista y el cuestionario, elaborado por el autor de la investigación, se recopiló información sobre cada una de las dimensiones de cada variable, las preguntas están referidas a los aspectos concretos para recopilar datos.

3.4.2. Análisis estadístico

Se realizó utilizando el paquete estadístico SPSS 26.0 con el que se procesó los datos obtenidos a través de los cuestionarios, para luego hacer su respectiva interpretación, análisis y discusión sobre los cuadros y gráficos estadísticos. También nos permitió encontrar los resultados, contrastar las hipótesis para poder construir las conclusiones que son el resultado final de la investigación.

Capítulo IV. Resultados

4.1. Análisis de los resultados

4.1.1. Tablas y gráficos de niveles de las dimensiones de la variable Sistema de Gestión de Seguridad de la información.

Tabla 6

Niveles de Integridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 3 – 6	08	16,3	16,3	16,3
	Medio 7 - 10	21	42,9	42,9	59,2
	Alto 11 - 15	20	40,8	40,8	100,0
	Total	49	100,0	100,0	

Fuente: Elaboración propia.

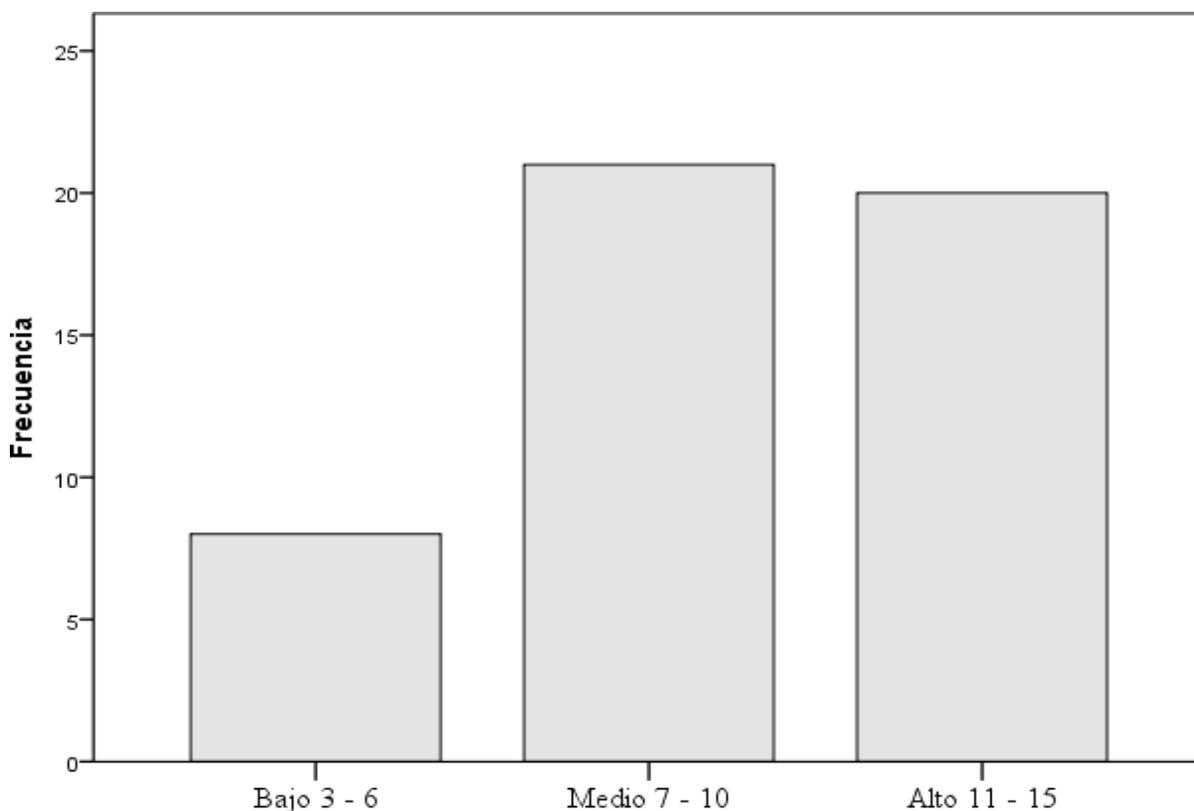


Figura 2. Niveles de Integridad de la información

Fuente: Elaboración propia.

La dimensión Integridad de la información tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo ≤ 6 , medio 7 - 10 y alto 11 - 15. De los 49 datos, el 16,3% de los trabajadores calificó la dimensión integridad de la información en un nivel bajo, el 42,9% en un nivel medio y el 40,8% en un nivel alto, obteniendo la mayor dispersión en el nivel medio.

Tabla 7
Niveles de Disponibilidad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 3 - 6	13	26,5	26,5	26,5
	Medio 7 - 10	24	49,0	49,0	75,5
	Alto 11 - 15	12	24,5	24,5	100,0
	Total	49	100,0	100,0	

Fuente: Elaboración propia.

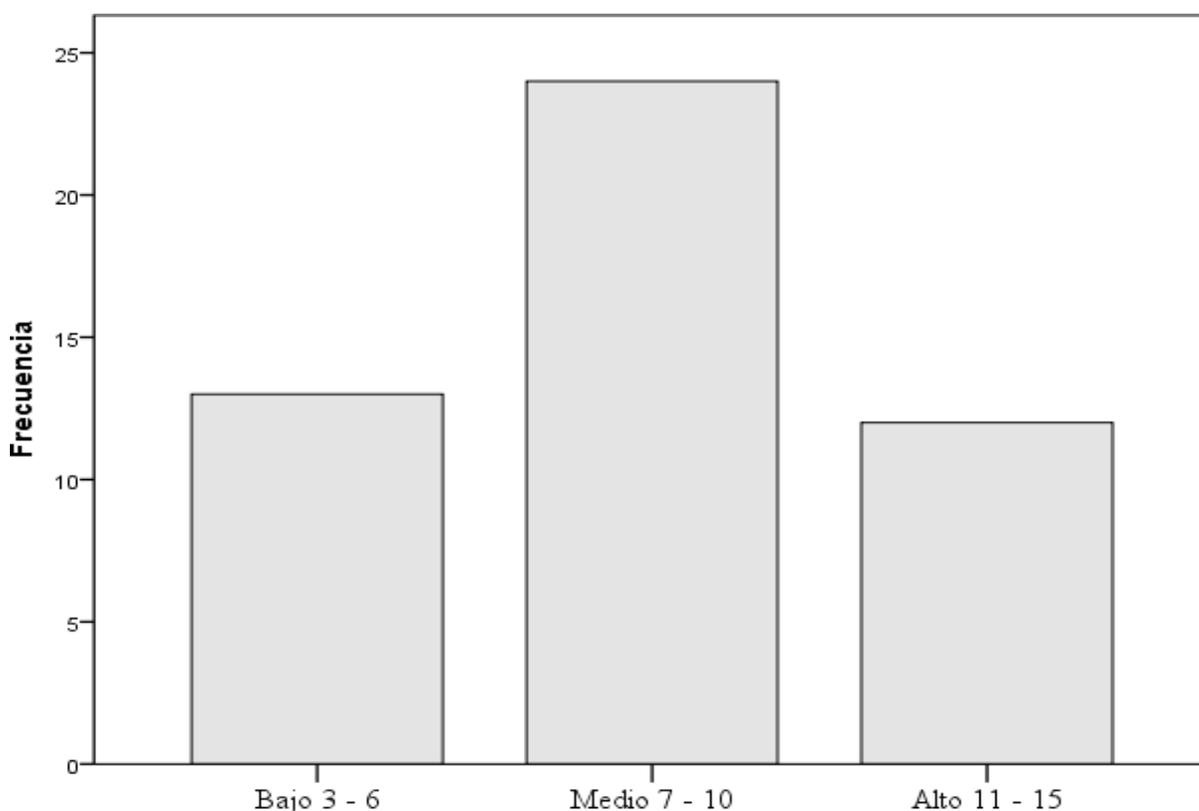


Figura 3. Niveles de Disponibilidad de la información

Fuente: Elaboración propia.

La dimensión Disponibilidad de la información tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo ≤ 6 , medio 7 - 10 y alto 11 - 15. De los 49 datos, el 26,5% de los trabajadores calificó la dimensión disponibilidad de la información en un nivel bajo, el 49,0% en un nivel medio y el 24,5% en un nivel alto, obteniendo la mayor dispersión en el nivel medio.

Tabla 8

Niveles de Confidencialidad de la información

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3 - 6	24	49,0	49,0	49,0
	Medio	7 - 10	11	22,4	22,4	71,4
	Alto	11 - 15	14	28,6	28,6	100,0
	Total		49	100,0	100,0	

Fuente: Elaboración propia.

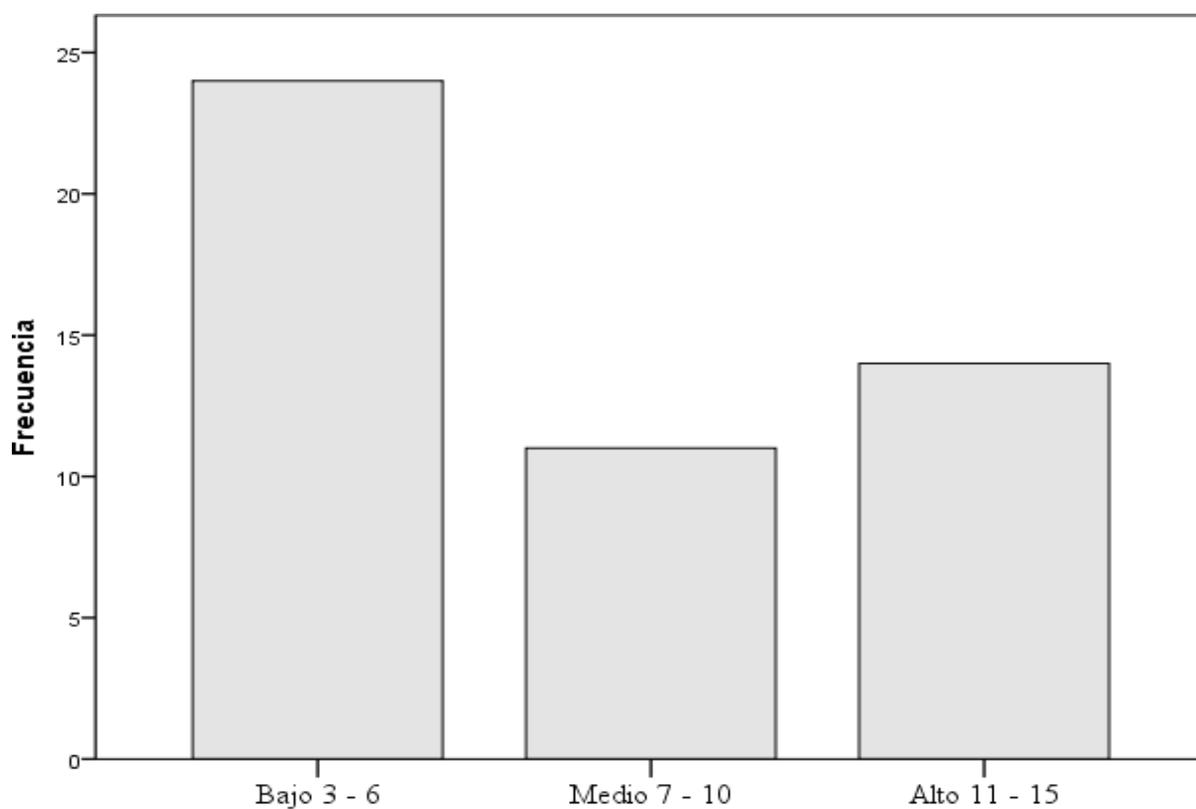


Figura 4. Niveles de Confidencialidad de la información

Fuente: Elaboración propia.

La dimensión Confidencialidad de la información tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo ≤ 6 , medio 7 - 10 y alto 11 - 15. De los 49 datos, el 49,0% de los trabajadores calificó la dimensión confidencialidad de la información en un nivel bajo, el 22,4% en un nivel medio y el 28,6% en un nivel alto, obteniendo la mayor dispersión en el nivel bajo.

4.1.2. Tablas y gráficos de niveles de las dimensiones de la variable Calidad de servicio.

Tabla 9
Niveles de Fiabilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 2 - 4	16	32,7	32,7	32,7
	Medio 5 - 7	9	18,3	18,3	51,0
	Alto 8 - 10	24	49,0	49,0	100,0
	Total	49	100,0	100,0	

Fuente: Elaboración propia.

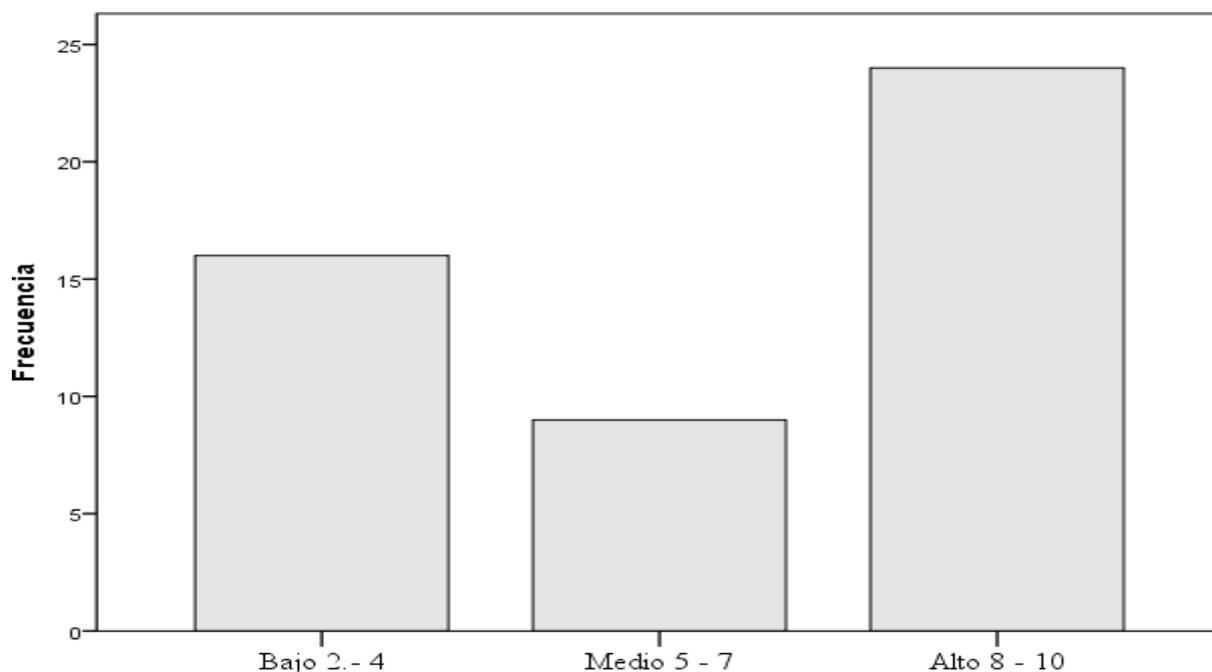


Figura 5. Niveles de Fiabilidad

Fuente: Elaboración propia.

La dimensión Fiabilidad tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo ≤ 4 , medio 5 - 7 y alto 8 - 10. De los 49 datos, el 32,7% de los trabajadores calificó la dimensión fiabilidad en un nivel bajo, el 18,3% en un nivel medio y el 49,0% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

Tabla 10
Niveles de Capacidad de respuesta

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 2 - 4	11	22,4	22,4	22,4
	Medio 5 - 7	29	59,2	59,2	81,6
	Alto 8 - 10	9	18,4	18,4	100,0
	Total	49	100,0	100,0	

Fuente: Elaboración propia.

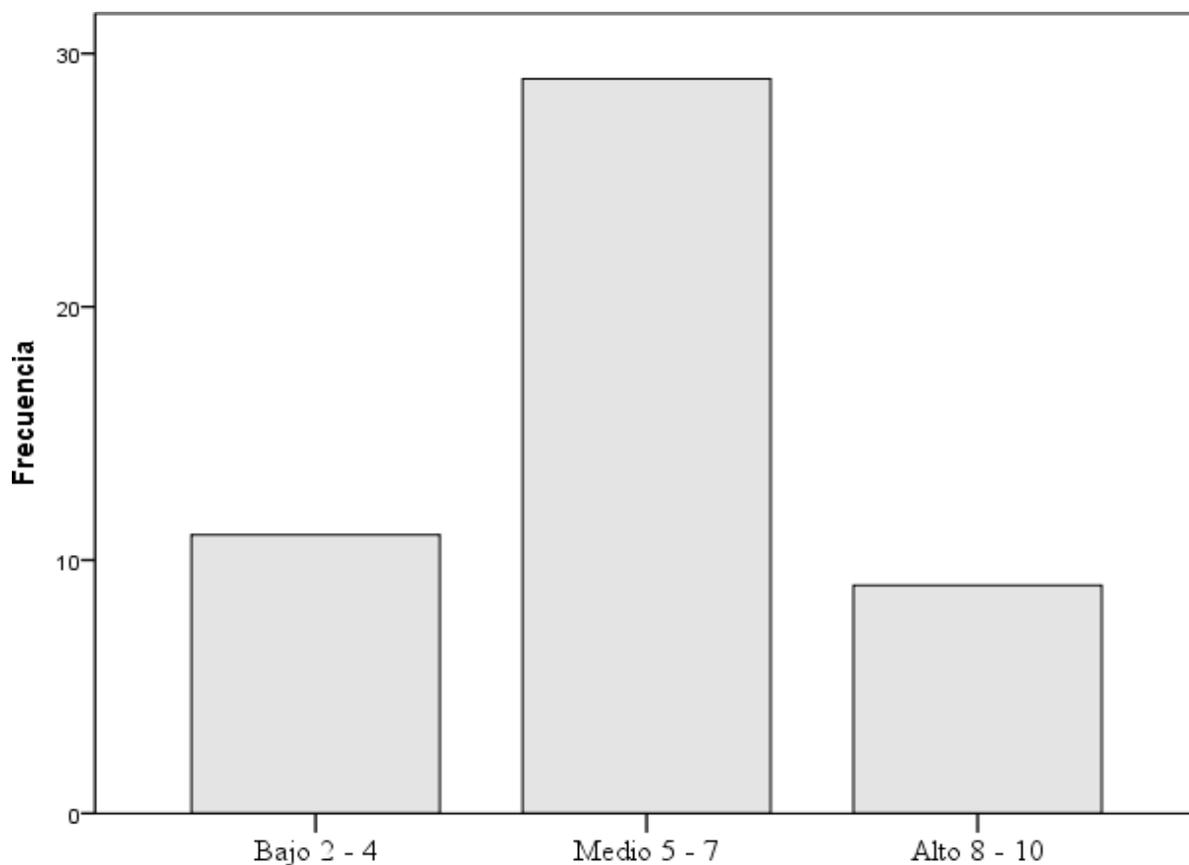


Figura 6. Niveles de Capacidad de respuesta

Fuente: Elaboración propia.

La dimensión Capacidad de respuesta tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo ≤ 4 , medio 5 - 7 y alto 8 - 10. De los 49 datos, el 22,4% de los trabajadores calificó la dimensión capacidad de respuesta en un nivel bajo, el 59,2% en un nivel medio y el 18,4% en un nivel alto, obteniendo la mayor dispersión en el nivel medio.

Tabla 11
Niveles de Tangibilidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido Bajo 3 - 6	6	12,2	12,2	12,2
Medio 7 - 10	6	12,3	12,3	24,5
Alto 11 - 15	37	75,5	75,5	100,0
Total	49	100,0	100,0	

Fuente: Elaboración propia.

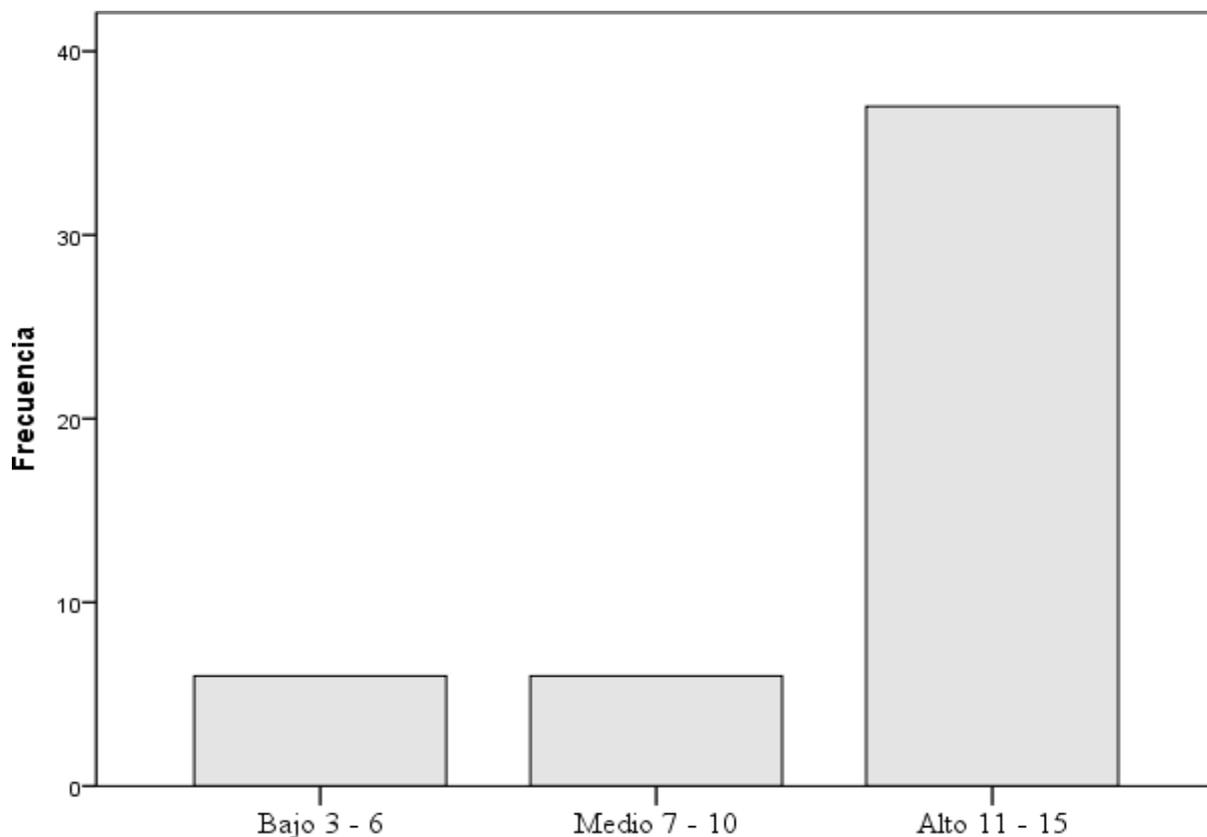


Figura 7. Niveles de Tangibilidad

Fuente: Elaboración propia.

La dimensión Tangibilidad tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo ≤ 6 , medio 7 - 10 y alto 11 - 15. De los 49 datos, el 12,2% de los trabajadores calificó la dimensión tangibilidad en un nivel bajo, el 12,3% en un nivel medio y el 75,5% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

4.1.3. Prueba de normalidad.

Planteamos la hipótesis de normalidad:

Ho: La distribución de la muestra sigue una distribución normal.

H1: La distribución de la muestra no sigue una distribución normal.

Establecemos el nivel de significancia:

El nivel de significancia establecido es de 0,05 y el nivel de confianza es de 95%.

Establecemos la regla de decisión:

Si $p < 0,05$: Se rechaza Ho

Si $p > 0,05$: Se acepta Ho

Elección de la prueba estadística:

Como prueba estadística se eligió el Test de Shapiro - Wilk porque es aplicada para muestras menores o iguales a 50 ($n \leq 50$), y en el caso de la presente investigación la muestra es igual a 49.

4.1.3.1. Calcular la nueva significación de las variables Sistema de gestión de seguridad de la información y Calidad de servicio.

Al utilizar el SPSS, hallamos las nuevas significancias:

Tabla 12

Prueba de normalidad de las variables Sistemas de gestión de seguridad de la información y Calidad de servicio

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Sistema de gestión de seguridad de la información	,950	49	,038
Calidad de servicio	,886	49	,000

Fuente: Elaboración propia.

Decisión:

Nueva significancia de la variable Sistema de gestión de la información = 0,038

$0,038 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Nueva significancia de la variable Calidad de servicio = 0,000

$0,000 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Interpretación:

Tomamos el estadístico de Shapiro - Wilk, porque la muestra es de 49 trabajadores, el cual muestra unas significancias de ambas variables menores que 0,05 por lo que se rechaza la hipótesis H_0 y se acepta la hipótesis H_1 , eso indica que la muestra no tiene distribución de probabilidad normal, por lo que concluimos con que el análisis debe utilizar pruebas no paramétricas.

4.1.3.2. Calcular la nueva significación de las dimensiones de la variable Sistemas de gestión de seguridad de la información.

Al utilizar el SPSS, hallamos las nuevas significancias:

Tabla 13

Prueba de normalidad de las dimensiones de la variable Sistemas de gestión de seguridad de la información

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Integridad de la información	,876	49	,000
Disponibilidad de la información	,889	49	,000
Confidencialidad de la información	,892	49	,000

Fuente: Elaboración propia.

Decisión:

Nueva significancia de la dimensión Integridad de la información = 0,000

$0,000 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Nueva significancia de la dimensión Disponibilidad de la información = 0,000

$0,000 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Nueva significancia de la dimensión Confidencialidad de la información = 0,000

$0,000 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Interpretación:

Tomamos el estadístico de Shapiro - Wilk, porque la muestra es de 49 trabajadores, el cual muestra unas significancias de las dimensiones de la variable Sistema de gestión de seguridad de la información menores que 0,05 por lo que se rechaza la hipótesis H_0 y se acepta la hipótesis H_1 , eso indica que la muestra no tiene distribución de probabilidad normal, por lo que concluimos con que el análisis debe utilizar pruebas no paramétricas.

4.1.3.3. Calcular la nueva significación de las dimensiones de la Calidad de servicio.

Al utilizar el SPSS, hallamos las nuevas significancias:

Tabla 14

Prueba de normalidad de las dimensiones de la variable Calidad de servicio

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Fiabilidad	,822	49	,000
Capacidad de respuesta	,921	49	,003
Tangibilidad	,888	49	,000

Fuente: Elaboración propia.

Decisión:

Nueva significancia de la dimensión Fiabilidad = 0,000

$0,000 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Nueva significancia de la dimensión Capacidad de respuesta = 0,003

$0,003 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Nueva significancia de la dimensión Tangibilidad = 0,000

$0,000 < 0,05$ se rechaza H_0 , demostrando que la distribución de la muestra no sigue una distribución normal.

Interpretación:

Tomamos el estadístico de Shapiro - Wilk, porque la muestra es de 49 trabajadores, el cual muestra unas significancias de las dimensiones de la variable Calidad de servicio menores que 0,05 por lo que se rechaza la hipótesis H_0 y se acepta la hipótesis H_1 , eso indica que la muestra no tiene distribución de probabilidad normal, por lo que concluimos con que el análisis debe utilizar pruebas no paramétricas.

4.2. Contrastación de hipótesis

4.2.1. Hipótesis general.

Formulación de hipótesis para contrastar:

H_1 : El sistema de gestión de seguridad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

H_0 : El sistema de gestión de seguridad de la información no se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra no sigue una distribución normal, se eligió el modelo de correlación de Rho de Spearman como prueba estadística para poder establecer si existe una relación entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 15
Correlación entre ambas variables

			Sistema de gestión de seguridad de la información	Calidad de servicio
Rho de Spearman	Sistema de gestión de seguridad de la información	Coeficiente de correlación	1,000	,780*
		Sig. (bilateral)	.	,000
		N	49	49
	Calidad de servicio	Coeficiente de correlación	,780*	1,000
		Sig. (bilateral)	,000	.
		N	49	49

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,780 y un Valor p = 0,000

Toma de la decisión:

Como regla de decisión se estableció que si el valor $p < 0,05$ se acepta H_1 y se rechaza H_0 . Como el valor $p = 0,000$ y $0,000 < 0,05$ se acepta la H_1 y se rechaza la H_0 .

Interpretación del p-valor:

Como el valor $p = 0,000$ y $0,000 < 0,05$ se afirma, con un 95% de confianza, que el sistema de gestión de seguridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, obteniendo una correlación positiva alta de 0,780.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor $p = 0,000$ y ser menor a 0,05 teniendo una correlación positiva alta de 0,780 por lo que se acepta H_1 , por lo tanto, se puede afirmar que el sistema de gestión de seguridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

4.2.2. Hipótesis específica 1.

Formulación de hipótesis para contrastar:

H_1 : La integridad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

H_0 : La integridad de la información no se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra no sigue una distribución normal, se eligió el modelo de correlación de Rho de Spearman como prueba estadística para poder establecer si existe una relación entre la integridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 16

Correlación entre la integridad de la información y la calidad de servicio

			Integridad de la información	Calidad de servicio
Rho de Spearman	Integridad de la información	Coeficiente de correlación	1,000	,830*
		Sig. (bilateral)	.	,000
		N	49	49
	Calidad de servicio	Coeficiente de correlación	,830*	1,000
		Sig. (bilateral)	,000	.
		N	49	49

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,830 y un Valor $p = 0,000$

Toma de la decisión:

Como regla de decisión se estableció que si el valor $p < 0,05$ se acepta H1 y se rechaza H0. Como el valor $p = 0,000$ y $0,000 < 0,05$ se acepta la H1 y se rechaza la H0.

Interpretación del p-valor:

Como el valor $p = 0,000$ y $0,000 < 0,05$ se afirma, con un 95% de confianza, que la integridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, obteniendo una correlación positiva alta de 0,830.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor $p = 0,000$ y ser menor a 0,05 teniendo una correlación positiva alta de 0,830 por lo que se acepta H1, por lo tanto, se puede afirmar que la integridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

4.2.3. Hipótesis específica 2.

Formulación de hipótesis para contrastar:

H1: La disponibilidad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

H0: La disponibilidad de la información no se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra no sigue una distribución normal, se eligió el modelo de correlación de Rho de Spearman como prueba estadística para poder establecer si existe una relación entre la disponibilidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 17

Correlación entre la disponibilidad de la información y la calidad de servicio

			Disponibilidad de la información	Calidad de servicio
Rho de Spearman	Disponibilidad de la información	Coefficiente de correlación	1,000	,887*
		Sig. (bilateral)	.	,000
		N	49	49
	Calidad de servicio	Coefficiente de correlación	,887*	1,000
		Sig. (bilateral)	,000	.
		N	49	49

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,887 y un Valor $p = 0,000$

Toma de la decisión:

Como regla de decisión se estableció que si el valor $p < 0,05$ se acepta H_1 y se rechaza H_0 . Como el valor $p = 0,000$ y $0,000 < 0,05$ se acepta la H_1 y se rechaza la H_0 .

Interpretación del p-valor:

Como el valor $p = 0,000$ y $0,000 < 0,05$ se afirma, con un 95% de confianza, que la disponibilidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, obteniendo una correlación positiva alta de 0,887.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor $p = 0,000$ y ser menor a 0,05 teniendo una correlación positiva alta de 0,887 por lo que se acepta H_1 , por lo tanto, se puede afirmar que la disponibilidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

4.2.4. Hipótesis específica 3.

Formulación de hipótesis para contrastar:

H_1 : La confidencialidad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

H_0 : La confidencialidad de la información no se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H_0 . El resultado será más significativo cuanto menor sea el valor P .

Elección de la prueba estadística:

Debido a que la distribución de la muestra no sigue una distribución normal, se eligió el modelo de correlación de Rho de Spearman como prueba estadística para poder establecer si existe una relación entre la confidencialidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 18

Correlación entre la confidencialidad de la información y la calidad de servicio

			Confidencialidad de la información	Calidad de servicio
Rho de Spearman	Confidencialidad de la información	Coefficiente de correlación	1,000	,658*
		Sig. (bilateral)	.	,000
		N	49	49
	Calidad de servicio	Coefficiente de correlación	,658*	1,000
		Sig. (bilateral)	,000	.
		N	49	49

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,658 y un Valor $p = 0,000$

Toma de la decisión:

Como regla de decisión se estableció que si el valor $p < 0,05$ se acepta H_1 y se rechaza H_0 . Como el valor $p = 0,000$ y $0,000 < 0,05$ se acepta la H_1 y se rechaza la H_0 .

Interpretación del p-valor:

Como el valor $p = 0,000$ y $0,000 < 0,05$ se afirma, con un 95% de confianza, que la confidencialidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, obteniendo una correlación positiva moderada de 0,658.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor $p = 0,000$ y ser menor a 0,05 teniendo una correlación positiva moderada de 0,658 por lo que se acepta H_1 , por lo tanto, se puede afirmar que la confidencialidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Capítulo V. Discusión

5.1. Discusión de resultados

En este capítulo se tuvo en cuenta a las investigaciones de los trabajos que sirvieron como base y antecedentes a la presente investigación y también a las conclusiones a las que llegaron sus diferentes autores.

En esta investigación queda demostrado estadísticamente que existe una relación positiva alta entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, con un 95% de probabilidad, un coeficiente de correlación de 0,780 y una significancia de 0,000 coincidiendo con la investigación de Sánchez (2023) quien realizó una investigación llamada “Seguridad de la información y calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión”, quien determinó que, existe una correlación alta entre el Sistema de gestión de seguridad de la información y la calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión, hallando un valor del coeficiente de correlación de $r = 0,881$; coincidiendo también con la investigación de Vergara (2017) quien en su investigación titulada “Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016”.concluye con que existe una relación directa y significativa de nivel moderado entre la seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016, obteniendo como resultado Rho de Spearman = 0.683** y un p-valor =0.000.

Este trabajo de investigación coincide, además, con la investigación de Elorrieta (2022) titulada “Desarrollo de un Sistema de gestión de seguridad de la información para bibliotecas basado en una metodología mejorada de análisis de riesgos compatible con la norma ISO/IEC 27001:20 Sistema de gestión de seguridad de la información y la calidad de servicio informático en la Universidad José Carlos Mariátegui, año 2019” en que concluye que existe

una relación entre el Sistema de Gestión de Seguridad de la Información (SGSI) y la Calidad del Servicio de tecnología de información, lo que ayuda a ver la situación actual en el proceso de seguridad, permitiendo aumentar su rendimiento al garantizar la seguridad, confiabilidad y disponibilidad de la información.

Coincide con la investigación de Pacheco (2021) titulada “Implementación de un sistema de gestión de calidad aplicando la norma ISO 9001:2015 ISO-IEC para mejorar la gestión administrativa de la Empresa Naylamp Ingenieros S.A.C.” en que con la implementación del sistema de gestión de calidad se mejora la gestión administrativa, evidenciándose en el incremento del conocimiento y aplicación de la norma en sus actividades diarias; y con la investigación de Zarbe (2019) quien desarrolló una tesis llamada “Sistema de gestión de seguridad de la información para la calidad de procesos en la I.E.P. Albert Einstein” quien llegó a la conclusión de que se mejora la seguridad de la información y los activos de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información.

Con la investigación de Bravo (2018) titulada “Desarrollo de un Sistema de gestión de seguridad de la información para bibliotecas basado en una metodología mejorada de análisis de riesgos compatible con la norma ISO/IEC 27001:2013” y con la de Esguerra y Ortiz (2018) titulada “Propuesta de implementación de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001:2013 para la empresa Lovato City Gas S.A.S” coincidimos con que, es vital implementar un sistema de gestión de seguridad de la información, debido a que logra identificar activos no inventariados, amenazas inminentes y riesgos potenciales, con el fin de gestionar y mantener un control adecuado sobre la información y procesos que maneja la empresa, donde se establecieron un conjunto de políticas de seguridad de la información las cuales mejorarán la protección, desempeño y efectividad a los procesos de la empresa, con lo que le permite alcanzar eficiencia en la administración de los recursos de una organización,

además proporciona mecanismos de protección y optimización de los recursos que se fundamentan en un ciclo de mejora continua.,

Con Guerra (2020), quien desarrolló una tesis llamada “Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la biblioteca de la Universidad de la Costa” y con Olivera (2019) quien realizó un trabajo de investigación llamado “Procedimiento para implementar un sistema de seguridad de la información como contribución a la calidad de la información de los servicios de consultoría. Aplicación en el Ciget de Holguín”, coincidimos con que el sistema de gestión de seguridad de la información es importante dentro de la empresa porque logra identificar los riesgos asociados a cada proceso, así como conocer el nivel de su impacto para ser evaluado, de acuerdo a las amenazas y vulnerabilidades, además permite implementar controles para reducir o mitigar los riesgos para los procesos de calidad, además permite elevar la cultura de gestión de seguridad por parte de los trabajadores y determinar nuevas competencias de formación de los mismos; redefinir los roles y responsabilidades de seguridad; evaluar la organización con relación a los requisitos de la Norma ISO/IEC 27001:2016 y del marco regulatorio asociado y obtener un inventario total de los activos de información de la organización.

Capítulo VI. Conclusiones y recomendaciones

6.1. Conclusiones

Podemos afirmar que el sistema de gestión de seguridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, debido a que los resultados que obtuvimos demuestran, con un 95% de probabilidad, que si existe una correlación positiva alta entre ambas variables ($R= 0,780$; $p=0,000 < 0,05$).

Podemos afirmar que la integridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, debido a que los resultados que obtuvimos demuestran, con un 95% de probabilidad, que si existe una correlación positiva alta de 0,830 entre ambos.

Podemos afirmar que la disponibilidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, debido a que los resultados que obtuvimos demuestran, con un 95% de probabilidad, que si existe una correlación positiva alta de 0,887 entre ambos.

Podemos afirmar que la confidencialidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, debido a que los resultados que obtuvimos demuestran, con un 95% de probabilidad, que si existe una correlación positiva moderada de 0,658 entre ambos.

6.2. Recomendaciones

Debido a que se llegó a la conclusión de que el sistema de gestión de seguridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, se recomienda supervisar constantemente el cumplimiento de los procedimientos y controles de seguridad de la información implementados para la calidad de servicios que brinda la empresa, de este modo, se garantiza un óptimo desempeño de las actividades dentro de la organización, al minimizarse los incidente contra la información.

Debido a que se llegó a la conclusión de que la integridad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, se recomienda realizar de forma constante, capacitación al personal acerca del uso correcto de los controles y procedimientos para el óptimo manejo de la información, evitándose o reduciendo de esta manera, los incidentes contra la integridad de la información ocasionados involuntariamente por el propio personal, o que puedan ser ocasionados por ataques informáticos por no cumplirse con los procedimientos de seguridad de la información.

Debido a que se llegó a la conclusión de que la disponibilidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, se recomienda dar mantenimiento a los diferentes equipos, dispositivos, sistemas de información y a la red con la que se trata y procesa la información, además deben contar con planes de contingencia, de esta manera se puede garantizar la disponibilidad de la información de forma continua.

Debido a que se llegó a la conclusión de que la confidencialidad de la información se relaciona con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023, se recomienda actualizar y capacitar al personal que trabaja con información estratégica o sensible, acerca de

los procedimientos y controles para el cuidado de la información, así como también sobre la legislación nacional relacionada con la protección de datos personales, de tal manera que se garantice la confidencialidad de la información.

Capítulo VII. Referencias

7.1. Fuentes bibliográficas

- Arias, E. (2019). *Plan de mejoramiento de la calidad del servicio y satisfacción de los usuarios del Gobierno Autónomo Descentralizado Municipal de Sucumbíos por el periodo septiembre 2018 – febrero 2019* (Tesis de pregrado). Universidad Central del Ecuador, Quito, Ecuador.
- Bravo, F. (2018). *Los sistemas de gestión y calidad de servicio de la empresa EPS Barranca S.A.* (Tesis de posgrado). Universidad Nacional José Faustino Sánchez Carrión, Huacho, Perú.
- Bravo, M. (2018). *Desarrollo de un sistema de gestión de seguridad de la información para bibliotecas basado en una metodología mejorada de análisis de riesgos compatible con la norma ISO/IEC 27001:2013* (Tesis de posgrado). Escuela Politécnica Nacional, Quito, Ecuador.
- Cáceda, C. (2021). *Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación* (Tesis de posgrado). Universidad Nacional Mayor de San Marcos, Lima, Perú.
- Cacuango, S. (2019). *Evaluación de una red LAN para el establecimiento de las Políticas de la Calidad de Servicio* (Tesis de posgrado). Universidad Tecnológica Israel, Quito, Ecuador.
- Castro, J. (2018). *Implementación de la NTP ISO/IEC 27001:2014 para mejorar la gestión de la seguridad en los sistemas de información de la autoridad Portuaria Nacional, Callao - 2017* (Tesis de pregrado). Universidad Autónoma del Perú, Lima, Perú.

- Ccesa, M. (2017). *Diseño de un sistema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016* (Tesis de pregrado). Universidad Nacional de San Cristóbal de Huamanga, Ayacucho, Perú.
- Elorrieta, H. (2022). *Sistema de gestión de seguridad de la información y la calidad de servicio informático en la Universidad José Carlos Mariátegui, año 2019* (Tesis de posgrado). Universidad José Carlos Mariátegui, Moquegua, Perú.
- Esguerra, L. y Ortiz, G. (2018). *Propuesta de implementación de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001:2013 para la empresa Lovato City Gas S.A.S* (Tesis de pregrado). Universidad Distrital Francisco de Caldas, Bogotá, Colombia.
- Godoy, R. (2014). Seguridad de Información. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.
- Guerra, E. (2020). *Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la Biblioteca de la Universidad de la Costa* (Tesis de pregrado). Universidad de la Costa, Barranquilla, Colombia.
- Maquera, G. (2022). *Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes Lan en la Municipalidad Distrital de Ilabaya* (Tesis de pregrado). Universidad Privada de Tacna, Tacna, Perú.
- Méndez, M. (2021). *Diseño de un sistema gestión de seguridad de información para proteger los activos de información del servicio de administración tributaria de la zona norte del Perú* (Tesis de posgrado). Universidad Privada del Norte, Trujillo, Perú.

- Narro, S. (2021). *El sistema de gestión de seguridad de la información y la gestión de riesgos en el área informática de una universidad pública, Región Cajamarca 2020* (Tesis de posgrado). Universidad Privada del Norte, Trujillo, Perú.
- NC ISO/IEC 27000:2016. (2016). *Tecnologías de la Información -Técnicas de Seguridad -Seguridad de Gestión de Seguridad de la Información (SGSI)- Visión de Conjunto y Vocabulario*. Cuba: Oficina Nacional de Normalización.
- NC ISO/IEC 27001:2016. (2016). *Tecnologías de la Información -Técnicas de Seguridad -Seguridad de Gestión de Seguridad de la Información (SGSI)- Requisitos*. Cuba: Oficina Nacional de Normalización.
- Olivera, Y. (2019). *Procedimiento para implementar un sistema de seguridad de la información como contribución a la calidad de la información de los servicios de consultoría. Aplicación en el Ciget de Holguín* (Tesis de posgrado). Universidad de Holguín, Holguín, Cuba.
- Osorio, L. (2016). *Gestión de Riesgos de Seguridad de la Información en el Sector Público*. Universidad Piloto de Colombia, Bogotá, Colombia.
- Pacheco, B. (2021). *Implementación de un sistema de gestión de calidad aplicando la norma ISO 9001:2015 ISO-IEC para mejorar la gestión administrativa de la Empresa Naylamp Ingenieros S.A.C.* (tesis de pregrado). Universidad Continental, Lima, Perú.
- Retuerto, A. (2017). *El compromiso organizacional y la calidad de servicio de los trabajadores de la municipalidad del distrito de Comas en el año 2016* (tesis de posgrado). Universidad Cesar Vallejo, Lima, Perú.
- Sánchez, E. (2023). *Seguridad de la información y calidad de servicio en la Universidad Nacional José Faustino Sánchez Carrión* (tesis de pregrado). Universidad Nacional José Faustino Sánchez Carrión, Huacho, Perú.

- Sandoval, J. (2017). *Diseño de un plan de seguridad de la información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, periodo 2015.2018* (Tesis de pregrado). Universidad Nacional de Piura, Piura, Perú.
- Torres, M. (2018). *Diseño de un sistema de seguridad de información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio Post-Venta de un integrador de soluciones en Telecomunicaciones* (tesis de pregrado). Universidad Peruana de Ciencias Aplicadas, Lima, Perú.
- Trinidad, M. (2019). *Sistema de Información Gerencial y la Gestión Administrativa de la Institución Educativa Honores del distrito de San Martín de Porres, 2018* (tesis de posgrado). Universidad Peruana de las Américas, Lima, Perú.
- Trujillo, W. (2020). *Diseño de controles y políticas para la seguridad de la información en la red Lan en el Hotel Pipatón* (Tesis de pregrado). Universidad Nacional Abierta y a Distancia - UNAD, Santander, Colombia.
- Vergara, G. (2017). *Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016* (tesis de posgrado). Universidad Nacional Federico Villarreal, Lima, Perú.
- Zarbe, R. (2019). *Sistema de gestión de seguridad de la información para la calidad de procesos en la I.E.P. Albert Einstein* (tesis de pregrado). Universidad Nacional de Ucayali, Pucallpa, Perú.

7.2. Fuentes hemerográficas

- Arévalo, F., Cedillo, I., y Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica*, 1(2), 31-42.

7.3. Fuentes electrónicas

Norma ISO 27001 (2016). *Sistema de Gestión de Seguridad de Información (SGSI)*.

Recuperado de: <https://www.iso27000.es/>

ANEXOS

Anexo N°1: Matriz de consistencia

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO EN LA EMPRESA FIBERLUX S.A.C. – 2023

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODO Y TECNICAS
<p><u>Problema General</u> ¿Existe relación entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?</p>	<p><u>Objetivos General</u> Determinar la relación que existe entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p>	<p><u>Hipótesis General</u> El sistema de gestión de seguridad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p>	<p>Sistema de gestión de seguridad de la información (X)</p>	<p>X.1.- Integridad de la Información. X.2.- Disponibilidad de la Información. X.3.- Confidencialidad de la Información.</p>	<p>X.1.1.- Seguridad de la comunicación. X.1.2.- Gestión de incidentes. X.1.3.- Seguridad lógica. X.2.1.- Acceso a la información en el tiempo requerido. X.2.2.- Continuidad del negocio. X.2.3.- Procedimientos de respaldo. X.3.1.- Privacidad de la información. X.3.2.- Autenticación. X.3.3.- Autorización.</p>	<p>Población: 55 Trabajadores de la empresa. Muestra: 49 Trabajadores de la empresa. Nivel de la investigación: Correlacional. Tipo de investigación: La presente investigación desarrolla un estudio de tipo aplicado.</p>
<p><u>Problemas Específicos</u> 1. ¿Existe relación entre la integridad de la información y la calidad de servicio en la</p>	<p><u>Objetivos Específicos</u> 1. Determinar la relación que existe entre la integridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p>	<p><u>Hipótesis Específicos</u> 1. La integridad de la información se relaciona significativamente con la calidad de servicio en la</p>	<p>Calidad de servicio (Y)</p>	<p>Y.1.- Fiabilidad. Y.2.- Capacidad de respuesta.</p>	<p>Y.1.1.- Eficiencia. Y.1.2.- Eficacia. Y.2.1.- Tiempo de respuesta. Y.2.2.- Mejora continua.</p>	<p>Método de la investigación: Deductivo. Diseño de la investigación: No experimental de tipo Transversal.</p>

<p>empresa Fiberlux S.A.C. en el 2023?</p> <p>2. ¿Existe relación entre la disponibilidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?</p> <p>3. ¿Existe relación entre la confidencialidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023?</p>	<p>2. Determinar la relación que existe entre la disponibilidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p> <p>3. Determinar la relación que existe entre la confidencialidad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p>	<p>empresa Fiberlux S.A.C. en el 2023.</p> <p>2. La disponibilidad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p> <p>3. La confidencialidad de la información se relaciona significativamente con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.</p>		<p>Y.3.- Tangibilidad.</p>	<p>Y.3.1.- Infraestructura. Y.3.2.- Condiciones generales. Y.3.3.- Almacenamiento.</p>	<p>Estadístico de prueba: Spearman</p> <p>Instrumento: Cuestionario de encuesta.</p>
--	---	--	--	----------------------------	--	--

Anexo N°2: Instrumento de recolecta de datos

**UNIVERSIDAD NACIONAL****“JOSÉ FAUSTINO SÁNCHEZ CARRIÓN”****FACULTAD INGENIERÍA INDUSTRIAL,
SISTEMAS E INFORMÁTICA****Escuela Profesional de Ingeniería Informática**

Cuestionario para medir la relación entre el sistema de gestión de seguridad de la información y la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Estimado (a) trabajador, esperamos tu colaboración respondiendo con responsabilidad y honestidad, el presente cuestionario. Se agradece no dejar ninguna pregunta sin contestar.

El objetivo es, recopilar información, para conocer el sistema de gestión de seguridad de la información y su relación con la calidad de servicio en la empresa Fiberlux S.A.C. en el 2023.

Instrucciones: Lea cuidadosamente las preguntas y marque con un aspa(x) la escala que crea conveniente.

Escala valorativa.

Muy en desacuerdo	Algo en desacuerdo	Ni de acuerdo ni en desacuerdo	Algo de acuerdo	Muy de acuerdo
1	2	3	4	5

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (X)						
N°	X.1.- Integridad de la información	1	2	3	4	5
1	X.1.1.- ¿Se documentan, revisan y actualizan los procedimientos de forma adecuada, de tal manera que garantiza la integridad de la Seguridad de la información?					
2	X.1.2.- ¿Se gestionan los incidentes de seguridad de la información para evitar futuros ataques contra la integridad?					
3	X.1.3.- ¿La empresa cuenta con seguridad lógica para la protección de la integridad de la información?					
	X.2.- Disponibilidad de la información					
4	X.2.1.- ¿La seguridad de la información garantiza el acceso a la información en el tiempo requerido?					
5	X.2.2.- ¿La disponibilidad de la información garantiza que exista continuidad del negocio?					
6	X.2.3.- ¿Se realizan procedimientos de respaldo periódicamente que garantice no se pierda la información?					

X.3.- Confidencialidad de la información						
7	X.3.1.- ¿Las funciones y roles que garantizan la confidencialidad de la información están bien definidas?					
8	X.3.2.- ¿Es obligatorio la autenticación de los usuarios para acceder a la información, de tal manera que garantiza la confidencialidad de la información?					
9	X.3.3.- ¿Existe procedimientos para autorizar el acceso a la información y conservar la confidencialidad?					
CALIDAD DE SERVICIO (Y)						
Y.1.- Fiabilidad						
10	Y.1.1.- ¿La calidad de servicio de los sistemas de información en la empresa es eficiente?					
11	Y.1.2.- ¿ Los accesos a la información por medio de los sistemas de información son efectivos?					
Y.2.- Capacidad de respuesta						
12	Y.2.1.- ¿El tiempo de respuesta al requerimiento de información es aceptable?					
13	Y.2.2.- ¿La capacidad de respuesta permite un servicio de calidad logrando la mejora continua de la empresa?					
Y.3.- Tangibilidad						
14	Y.3.1.- ¿La infraestructura de la empresa es la adecuada para brindar una buena calidad de servicio?					
15	Y.3.2.- ¿Las condiciones generales permiten que exista una adecuada calidad del servicio?					
16	Y.3.3.- ¿Existe un adecuado almacenamiento en la empresa para brindar un servicio de calidad?					

Muchas gracias por tu colaboración

Anexo N°3: Fichas de validación de juicio de expertos.

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO

TÍTULO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO EN LA EMPRESA FIBERLUX S.A.C. EN EL 2023

AUTOR DEL INSTRUMENTO: BRUSELINO YUNIOR BLAS ZORRILLA

I. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente 0 - 20				Regular 21 - 40				Bueno 41 - 60				Muy Bueno 61 - 80				Excelente 81 - 100			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulado con lenguaje apropiado																				X
2. Objetividad	Está expresado en hechos observables																				X
3. Actualidad	Adecuado al avance de la tecnología.																	X			
4. Organización	Existe una organización lógica																				X
5. Suficiencia	Comprende los aspectos en cantidad y calidad																				X
6. Intencionalidad	Adecuado para valorar los aspectos del sistema de gestión de seguridad de la información y la calidad de servicio																				X
7. Consistencia	Basado en aspectos teóricos – científicos.																	X			
8. Coherencia	Establece coherencia entre las variables y los indicadores																				X
9. Metodología	La estrategia responde a los objetivos																				X
10. Pertinencia	Es útil y adecuado para la investigación																				X

II. OPINIÓN DE APLICABILIDAD: Proceda a su aplicación.

III. PROMEDIO DE VALORACIÓN: 89,0



Lugar y fecha: Lima, 10 de enero del 2024

Firma del Experto Informante
Apellidos y nombres: Figueroa Revilla, Jorge Martín
DNI N°066722809

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO

TÍTULO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO EN LA EMPRESA FIBERLUX S.A.C. EN EL 2023

AUTOR DEL INSTRUMENTO: BRUSELINO YUNIOR BLAS ZORRILLA

I. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente 0 - 20				Regular 21 - 40				Bueno 41 - 60				Muy Bueno 61 - 80				Excelente 81 - 100			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulado con lenguaje apropiado																			X	
2. Objetividad	Está expresado en hechos observables																			X	
3. Actualidad	Adecuado al avance de la tecnología.																			X	
4. Organización	Existe una organización lógica																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																			X	
6. Intencionalidad	Adecuado para valorar los aspectos del sistema de gestión de seguridad de la información y la calidad de servicio.																			X	
7. Consistencia	Basado en aspectos teóricos – científicos.																			X	
8. Coherencia	Establece coherencia entre las variables y los indicadores																	X			
9. Metodología	La estrategia responde a los objetivos																			X	
10. Pertinencia	Es útil y adecuado para la investigación																	X			

II. OPINIÓN DE APLICABILIDAD: Proceda a su aplicación.

III. PROMEDIO DE VALORACIÓN: 88,5

Lugar y fecha: Lima, 16 de enero del 2024



Firma del Experto Informante
 Apellidos y nombres: Flores Cueto, Juan José
 DNI N°09593196

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO DE LAS REDES

TÍTULO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE SERVICIO EN LA EMPRESA FIBERLUX S.A.C. EN EL 2023

AUTOR DEL INSTRUMENTO: BRUSELINO YUNIOR BLAS ZORRILLA

I. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente 0 - 20				Regular 21 - 40				Bueno 41 - 60				Muy Bueno 61 - 80				Excelente 81 - 100			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulado con lenguaje apropiado																	X			
2. Objetividad	Está expresado en hechos observables																		X		
3. Actualidad	Adecuado al avance de la tecnología.																		X		
4. Organización	Existe una organización lógica																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																		X		
6. Intencionalidad	Adecuado para valorar los aspectos del sistema de gestión de seguridad de la información y la calidad de servicio.																	X			
7. Consistencia	Basado en aspectos teóricos – científicos.																		X		
8. Coherencia	Establece coherencia entre las variables y los indicadores																		X		
9. Metodología	La estrategia responde a los objetivos																		X		
10. Pertinencia	Es útil y adecuado para la investigación																		X		

II. OPINIÓN DE APLICABILIDAD: Proceda a su aplicación.

III. PROMEDIO DE VALORACIÓN: 88,5

Lugar y fecha: Lima, 10 de enero del 2024

Firma del Experto Informante

Apellidos y nombres: Nicho Virú, Martín W.

DNI N°15759740

Anexo N°4: Tabla de datos en SPSS.

*Datos.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Marketing directo Gráficos Utilidades Ampliaciones Ventana Ayuda

Visible: 30 de 30 variables

	Items1	Items2	Items3	Items4	Items5	Items6	Items7	Items8	Items9	Items10	Items11	Items12	Items13	Items14	Items15	Items16
1	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
2	1	1	1	1	1	2	2	1	2	2	2	2	1	1	2	2
3	3	3	3	3	3	2	3	1	1	4	4	4	1	4	4	2
4	3	4	4	3	4	5	3	5	5	5	5	4	5	5	4	5
5	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
6	1	1	1	1	1	1	2	1	2	2	2	2	1	1	2	2
7	2	3	3	2	2	1	2	2	2	1	1	1	2	2	2	2
8	3	3	3	3	3	4	3	1	1	4	4	4	1	4	4	4
9	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
10	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2
11	3	4	4	3	4	5	3	5	5	5	5	4	5	5	4	5
12	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1
13	5	4	5	1	4	5	5	5	5	5	5	2	5	5	1	5
14	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
15	5	4	5	1	4	5	5	5	5	5	5	5	5	5	1	5
16	5	3	3	2	2	1	2	2	2	1	1	1	5	5	5	5
17	3	4	4	3	4	5	3	4	4	4	4	4	1	4	4	4
18	1	3	3	3	3	5	3	3	3	2	2	5	5	5	5	5
19	2	4	5	1	4	5	2	2	2	5	5	2	5	5	1	5
20	3	3	3	3	3	4	3	1	1	4	4	4	1	4	4	4
21	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
22	1	1	1	1	1	5	1	1	1	1	1	1	1	1	1	5

Vista de datos Vista de variables

IBM SPSS Statistics Processor está listo Unicode:ON



Visible: 30 de 30 variables

	Items1	Items2	Items3	Items4	Items5	Items6	Items7	Items8	Items9	Items10	Items11	Items12	Items13	Items14	Items15	Items16
23	3	4	4	3	4	5	3	4	4	4	4	4	1	4	4	4
24	3	4	4	3	4	5	3	2	2	5	5	4	5	5	4	5
25	2	3	3	2	2	1	2	2	2	1	1	1	5	5	5	5
26	2	4	5	1	4	5	2	2	2	5	5	2	5	5	1	5
27	1	1	1	1	1	5	1	1	1	1	1	1	1	1	1	5
28	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
29	2	4	5	1	4	5	2	2	2	5	5	5	5	5	1	5
30	2	3	3	2	2	1	2	2	2	1	1	1	5	5	5	5
31	3	4	4	3	4	5	3	4	4	4	4	4	1	4	4	4
32	5	4	4	3	4	5	5	5	5	5	5	2	5	5	4	5
33	2	3	3	2	2	2	2	2	2	1	1	1	2	2	2	4
34	3	3	3	3	3	4	3	1	1	4	4	4	1	4	4	4
35	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
36	1	1	1	1	1	1	2	1	2	2	2	2	2	2	2	2
37	3	4	4	3	4	5	3	5	5	5	5	4	5	5	4	5
38	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	3
39	5	4	5	4	4	5	5	5	5	5	5	2	5	5	1	5
40	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
41	5	4	5	3	4	5	5	5	5	5	5	5	5	5	1	5
42	2	3	3	2	2	1	2	2	2	1	1	1	5	5	5	5
43	2	4	5	1	4	5	2	2	2	5	5	2	5	5	1	5
44	3	4	4	3	4	5	3	5	5	5	5	4	5	5	4	5

*Datos.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Marketing directo Gráficos Utilidades Ampliaciones Ventana Ayuda

Visible: 30 de 30 variables

	Items1	Items2	Items3	Items4	Items5	Items6	Items7	Items8	Items9	Items10	Items11	Items12	Items13	Items14	Items15	Items16
45	5	4	5	1	4	5	5	5	5	5	5	2	5	5	1	5
46	5	4	5	1	4	5	5	5	5	5	5	2	5	5	1	5
47	2	3	3	2	2	2	2	2	2	1	1	1	2	2	2	4
48	3	3	3	3	3	4	3	1	1	4	4	4	1	4	4	4
49	3	3	3	3	3	3	4	3	3	4	3	4	1	4	4	3
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66

Vista de datos Vista de variables

IBM SPSS Statistics Processor está listo Uniq 6 notificaciones nuevas